2010-09-01

Cloud Computing:Strategies for Cloud Computing Adoption

Faith Shimba

Technological University Dublin, faith.shimba@gmail.com

School of Computing

Dissertations

Dublin Institute of Technology *Year* 2010

Cloud Computing:Strategies for Cloud Computing Adoption

Faith Shimba Mr.
Dublin Institute of Technology, faith.shimba@student.dit.ie

— Use Licence —

Attribution-NonCommercial-ShareAlike 1.0

You are free:

- to copy, distribute, display, and perform the work
- to make derivative works

Under the following conditions:

- Attribution.
  You must give the original author credit.
- Non-Commercial.
  You may not use this work for commercial purposes.
- Share Alike.
  If you alter, transform, or build upon this work, you may distribute the resulting work only under a license identical to this one.

For any reuse or distribution, you must make clear to others the license terms of this work. Any of these conditions can be waived if you get permission from the author.

Your fair use and other rights are in no way affected by the above.

Cloud Computing: Strategies for Cloud Computing Adoption

Faith Shimba

A dissertation submitted in partial fulfilment of the requirements of Dublin Institute of Technology for the degree of

M.Sc. in Computing (Information Technology)

September 2010

I certify that this dissertation which I now submit for examination for the award of MSc in Computing (Information Technology), is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the test of my work.

This dissertation was prepared according to the regulations for postgraduate study of the Dublin Institute of Technology and has not been submitted in whole or part for an award in any other Institute or University.

The work reported on in this dissertation conforms to the principles and requirements of the Institute's guidelines for ethics in research.

Signed: _____

Date: ***01 September 2010***

ABSTRACT

The advent of cloud computing in recent years has sparked an interest from different organisations, institutions and users to take advantage of web applications. This is a result of the new economic model for the Information Technology (IT) department that cloud computing promises. The model promises a shift from an organisation required to invest heavily for limited IT resources that are internally managed, to a model where the organisation can buy or rent resources that are managed by a cloud provider, and pay per use. Cloud computing also promises scalability of resources and on-demand availability of resources.

Although, the adoption of cloud computing promises various benefits to an organisation, a successful adoption of cloud computing in an organisation requires an understanding of different dynamics and expertise in diverse domains. Currently, there are inadequate guidelines for adopting cloud computing and building trust. Therefore, this research project aims at developing a roadmap called ROCCA (Roadmap for Cloud Computing Adoption), which provides organisations with a number of steps for adopting cloud computing and building trust. An associated framework called ROCCA Achievement Framework (RAF) is also proposed. RAF is a framework that uses the criteria in the ROCCA to build a framework for measuring the adherence level to the proposed roadmap.

This dissertation focuses on a range of strategic issues from a broad cross section of areas of expertise required to ensure a successful cloud computing adoption. It presents in detail the technological factors key to a successful cloud computing adoption, and it introduces the technology underlying cloud computing, and describes different cloud computing delivery and deployment models.

It explains how an emphasis on collaboration between clients and vendor is essential for successful adoption of cloud computing. If the organisation feels free, confident and secure to use cloud services then it is more likely that the adoption rate will increase. By following the guidelines outlined, organisations can ensure that their adoption of cloud computing are effective, efficient and provides a high degree of satisfaction. This dissertation also covers

cloud computing from a business perspective, ensuring that cloud computing adoption projects are fully costed, and risks are properly understood.

Key words*: Adoption, cloud, cloud computing, security, trust, ROCCA, RAF*

ACKNOWLEDGEMENTS

Writing an acknowledgement is not an easy. This is because there are so many people who have helped along the way. The authors' greatest fear is forgetting someone, so I start off by saying thank you to all. If your name is not mentioned, please forgive me!

Thanks go to Dr. Pierpaolo Dondio of the Distributed Computing Group, at Trinity College, who served as my supervisor during the course of writing this dissertation. Dr. Pierpaolo Dondio also helped greatly by providing critical directions whenever needed (of course if this dissertation is a mess the blame falls on me and only me!).

Thanks to Dr. Ronan Fitzpatrick for his challenging seminars and discussions during the taught part of this course and for his invaluable feedback in the preparation of this dissertation. Dr. Fredrick J. Mtenzi, for his never ending support and encouragement throughout the course of my studies. Mr. Wawila Mwazembe for providing the author with the case study outlined in chapter eight and feedback on the roadmap and framework proposed in this dissertation.

Special thanks to Zanifa Omary for sharing her experience in research and dissertation writing. I would be negligent if I did not mention my family, my parents Joel and Helena; and especially my Wife Irene and our boys Shalom and Jedidijah, who have supported me through the thick and thin of this MSc studies and Kenneth and Witness special kids.

Last but not least, all DT 230 lecturers and students for the different discussions, challenges and experiences shared during the taught part of this MSc. Course.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. INTRODUCTION

1.1 What is Cloud Computing?

Cloud computing is a new term in the computing world (Luis et al., 2008, Buyya et al., 2008) and it signals the advent of a new computing paradigm (Luis et al., 2008). This new paradigm is quickly developing and attracts a number of customers and vendors alike. The quick development of cloud computing is being fuelled by the emerging computing technologies which allows for reasonably priced use of computing infrastructures and mass storage capabilities. It also removes the need for heavy upfront investment in Information Technology (IT) infrastructure. Cloud computing is a computing paradigm that involves outsourcing of computing resources with the capabilities of expendable resource scalability, on-demand provisioning with little or no up-front IT infrastructure investment costs (Catteddu and Hogben, 2009, Chow et al., 2009, GNi, 2009, Jeffrey and Neidecker-Lutz, 2009). Cloud computing offers its benefits through three types of service or delivery models namely infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and software-as-a-Service (SaaS). It also delivers its service through four deployment models namely, public cloud, private cloud, community cloud and hybrid cloud (CSA, 2009).

1.2 Trust and Challenges in cloud computing adoption

Cloud computing adoption is faced with a number of challenges, these challenges are: security challenges, legal and compliance challenges and organisational challenges (Andrei, 2009, Buyya *et al.*, 2008, Catteddu and Hogben, 2009, Khajeh-Hosseini *et al.*, 2010a). Linked to all these challenges is the issue of trust between clients and vendors, because cloud computing calls for organisations to trust vendors with the management of their IT resources and data.

Trust being a critical factor in cloud computing adoption, this research project will focus specifically in identifying the challenges facing organisations when seeking to adopt cloud computing. Of all the challenges security has received more mention. This is because *"security is both a feeling and a reality. And they are not the same."* (Schneir, 2008). This means that the reality of security is tied to the probability of different risks and how effective are the strategies to mitigate the perceived risks are. Security is also a feeling in

that; it is based on the psychological reactions to both the risks and the countermeasures. Therefore, Cloud computing needs to appeal to both the feelings of the potential customers and address the reality of the risks associated with cloud computing in a way that customers will feel safe and secure to use cloud computing. This is what this project calls building customer trust. That is, the ability of cloud computing to appeal to both the feelings of potential customers and the reality of the security risks of cloud computing in a way that customers will feel safe and secure to use it.

Although there are no security breaches that have been reported, but the instances of cloud outages resulting in loss of service to customers increases the reluctance and fuels the fear of adopting cloud computing. Examples from the last two years are such as the March 13, 2009 Microsoft sidekick which lasted for six days, in this case Microsoft reported that there were customer data losses and attributed the loss to system failure. Another example is the Google Gmail in October 16, 2008, the outage affected Google apps customers resulting in failure to access applications such as emails. Another example is the Microsoft Azure in March 13, 2009 (Williams, 2010). A more recent example is salesforce.com outage which occurred in Janury 2010. In this case service to all 68,000 salesforce.com customers was disrupted but there was no reported data loss (Bingelow, 2010).

In order to build trust, cloud computing trust models need to be able to address the different challenges that are raised by cloud computing. This address should be as holistic as possible covering the different aspects of cloud computing. This means the trust model should address the different challenges raised in the different deployment and delivery models and provide a way for both customers and service providers to evaluate the trust level offered. A number of models exists that try to address the challenge in building trust between customer and cloud service providers. These models are: the trusted computing platform (TCCP) (Santos et al., 2009), Private virtual infrastructure (Krautheim, 2009), Cloud cube model (JERICHO, 2009) among others.

1.3 Research problem

Academic research on the adoption of cloud computing and in particular the building of customer trust is minimal and profuse. Some work has been done on the models of trust and adoption strategies for cloud computing. Security is a topic that is receiving increasing focus as adoption of cloud computing is considered. Industry publication points to the financial

benefits of adopting cloud computing and the costs of migrating to cloud computing. There is little published work on the legal and compliance considerations of adopting cloud computing, as well as, the organisational impact that cloud computing will have on the organisation.

This dissertation attempts to provide a suitable high level roadmap, which will provide organisations with a strategy for cloud computing adoption project. It discusses the security considerations, legal and compliance considerations, and organisational issues. Adopting cloud computing requires broad knowledge across diverse disciplines. It is useful to have a roadmap of the diverse areas that must be addressed

In order to explore the trust characteristics of the cloud vendors the following research questions are presented:

Question 1: what are the key barriers to cloud computing adoption?
Question 2: is it possible for client and vendor to collaborate for successful cloud adoption project?
Question 3: can a roadmap to address the challenges facing cloud computing adoption and successfully adopt cloud computing be developed?

And the following hypothesis is put forward: by using the developed roadmap, the CTOs, CIOs will have a better understanding of the key issues involved in cloud computing adoption and they will have a tool to guide the process for adoption.

1.4 Intellectual challenges

This research project will be among the few projects which have been carried out in the area of cloud computing security (CSA, 2009). Cloud computing technology has emerged recently (Armbrust et al., 2009, Wang and Laszewski, 2008) and there are few academic researches which have been done in the area of cloud computing research in general and trust in particular. An example of these research projects are the Eucalyptus (Nurmi et al., 2009) and Reservoir (Rochwerger et al., 2009), and on cloud computing trust research projects are such as the Trusted Cloud Computing Platform (TCCP) (Santos et al., 2009), Private Virtual Infrastructure (Krautheim, 2009) and the Cloud Cube Model (JERICHO, 2009), and for adoption strategies the cloud adoption toolkit (Greenwood *et al.*, 2010, Keene

et al., 2009). Therefore, the first challenge is the investigation and classification of literature from both the industry and the academia as it is still not comprehensive and mature.

Lack of a tool from the industry or academia that customers can use to measure vendors' claims for how trustworthy their offerings are is another challenge. Researchers have not provided the customers with a way of measuring the claims of the cloud service provider as to how trustworthy their clouds are. Challenges are in understanding what are the customers wants and what the current state of the art of cloud computing can provide.

A third challenge is that of lack of clear understanding from the literature/industry publications of what the customers' think/need or fear. A data collection effort using surveys, literature review and reports has to be produced, representing a challenging task.

The knowledge of the customer expectations and requirements must be well known as well as the type of services provided by cloud computing environment must be understood. This challenge will be worked out through efficient analysis and review of literature and data collection. To facilitate this, online questionnaires and an appropriate selection of sample space, that is, unbiased, and the use of suitable tools was used.

1.5 Research objectives

The principal aim of this dissertation is to investigate the primary strategic issues in adopting cloud computing in an organisation. Following on from this research a roadmap will be developed that can be used to guide organisations through the process of successfully adopting or migrating to cloud computing. This roadmap will serve as a guide to the different strategic issues that can help in evaluating, planning and migration to cloud computing. It is seen that the roadmap will be of use to Chief Information Officers (CTO), technical managers and management in general as it will combine both the strategic factors from a number of disciplines, namely security, legal and organisational management.

1.6 Research methodology

Extensive secondary research will be conducted. Acknowledged texts, standards documents, industry periodicals and white papers, analysts' reports and conference journals will be referenced. A critical analysis of the secondary research is applied in the formulation of the roadmap and framework proposed.

The data for this research will be collected from statements about privacy policy, acceptable use policy, terms of use and service level agreements available from the websites of the cloud vendors. In case of any such information missing from the websites, similar information will be sought via internet research of whitepapers, press releases and news articles of cloud computing in different IT magazines.

A set of cloud computing vendors will be chosen based on multiple online resources such as top 10 lists from Forrester research, focus, CIO's Cloud computing vendors to watch, Top 10 SaaS providers awards and scores assigned to vendors.

The research will focus on three categories of cloud computing service models, the vendor size and vendor online traffic to explore the customer trust level of cloud computing vendors. The three cloud computing service models are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

The evaluation of the proposed solution will be through the use of a case study and a walkthrough of the case study from the industry.

1.7 Resources

For a successful completion of this project a number of resources are required. The following is the list of the resources which will be required during the course of conducting the research project.

- Laptop computer for writing the dissertation and conducting the research project.
- Internet access, both at home and in DIT.
- Access to DIT library. This will enable easy access to a variety of academic resources such as journals and periodicals in both hard copy and electronic format.
- Access to DIT student account, for backup of the research project materials.
- Access to statistical tools. SurveyMonkey for online questionnaire and SPSS software for data analysis.

1.8 Scope and limitations

Since cloud computing is still maturing as a computing field, there is a plenty of research avenues and challenges that can be explored. These research areas are such as security, social-technical impact of cloud computing, business models among others. However, this

research project will focus on the challenge facing organisation in their endeavour to adopt cloud computing by identifying these challenges and propose a high level roadmap that will act as a guideline for technical and business managers when evaluating a cloud adoption project.

Nevertheless, there were a number of limitations that faced the project. The key limitation was the time to accomplish the research project. The three months period which was during the summer months was a limiting factor as it had effects on the amount of survey response and evaluation of the research outcome. It affected the survey response as only fifty percent of the survey invitations sent out received response, with the remaining fifty percent failing to take part as they were on summer holidays. As for the evaluation of the proposed solution, the researchers only managed to get one case study as most of the companies that could have provided researchers with more evaluation; their personnel were on summer holidays.

1.9 Organisation of the dissertation

The remaining chapters of this dissertation are organised as follows:

Chapter 2 focuses on the literature review of the cloud computing. It provides the definitions and key characteristics of cloud computing, the different delivery and service models of cloud computing.

Chapter 3 discusses the issues of trust in computer science. It provides the definition of trust, its characteristics and identifies areas of trust concerns in cloud computing.

Chapter 4 discusses a range of security, legal and compliance issues surrounding cloud computing adoption and building customer trust.

Chapter 5 discusses the organisational factors related to adopting cloud computing.

Chapter 6 discusses the survey results and provides the analysis of the results and its findings.

Chapter 7 brings together the critical factors from the previous three chapters into a roadmap, which provides strategy for adopting cloud computing.

Chapter 8 presents the research evaluation, and a walkthrough of a case study to show how the roadmap and its evaluation framework can be applied.

Chapter 9 summarises the research, provides conclusions and discusses further areas of research.

2. CLOUD COMPUTING

2.1 Introduction

The advent of cloud computing in recent years has sparked interest from different stakeholders of Information Technology (IT) and Computer science, such as academicians, business organisations, institutions. With its promise of a new economic model for the Computing/Communication and Information Technology (CIT) department of business organisation, cloud computing brings about a shift in the way organisation invest in their IT resources. The new economic model removes the need for the organisation to invest a substantial sum of money for purchase of limited IT resources that are internally managed, but rather the organisation can outsource its IT resource requirements to a cloud computing service provider and pay per use.

This new computing paradigm called cloud computing has also brought challenges to the organisation seeking to adopt it. The challenges that are raised are: trust, security, legal, compliance and organisational challenge. These challenges are closely linked to trust (chapter 3, 4 and 5).

This chapter provides the background material for the remainder of this dissertation. The first section provides the definition of cloud computing, a brief history of cloud computing, underlying technologies, service and delivery models offered by cloud computing and the benefits of using cloud computing. The second section will introduce the concepts of trust in computer systems and highlight different types of trust and how trust is built in computer systems. It will also identify the challenges in building trust in cloud computing and propose ways of building trust in cloud computing.

2.2 Cloud Computing

Without a doubt, the advent of cloud computing in recent years has sparked an interest from different stakeholders, business organisations, institutions and government agencies. This interest is fuelled by the promised new economic model of cloud computing which brings a shift from heavy IT infrastructure invest for limited resources that are internally managed and owned to pay per use for IT infrastructure owned by a service provider. Also, it promises scalability and on-demand provisioning of resources.

However the term cloud computing is fairly new since its emergence in the computing world (Luis et al., 2008). Although the term is new, its concepts are not new. Cloud computing borrows terms and concepts from other computing paradigms such as utility computing, grid computing, service oriented architecture among others (Luis et al., 2008, Wang and Laszewski, 2008, Geelan, 2009, Buyya et al., 2008). This shows that cloud computing has been in existence in different forms since the beginning of computing, and it can be traced back to early sixties. In the sixties timesharing and utility computing emerged. MULTICS was then the holy grail of computer science of the age (MIT, 2009). This project failed because it was far ahead of its time. There was no public Internet, lack of communication technology and high speed processing and storage capacities. It was during this era that, timesharing and multitasking – operating systems technology emerged. These technology were pre-cursors of cloud computing (Wang and Laszewski, 2008).

The seventies witnessed the mainframe era and with a company like Tymeshare Inc renting out storage space and processing power via the telephone line (Bhattacharjee, 2009). The Eighties saw the advent of personal computers, while the nineties saw the dot-com bubble and the advent of grid computing. Grid computing aimed at linking and enabling the sharing of computing resources, while the dot-com bubble led to the emergence of datacenters. Yet these datacenters were not fully utilised, and this led to the virtualisation technology, and thus the birth of modern day cloud computing (Bhattacharjee, 2009).

The first attempt at cloud computing were in 1999 when Marc Andreesen founded the LoudCloud company which was to "*build the web's next power play: custom-designed, infinitely scalable sites that blast off a virtual assembly line*" (Sheff, 2003). The company intended to be a managed service provider. It was the first company to offer services which are now called Software as a Service (SaaS) using an Infrastructure as a Service model (IaaS) (Sheff, 2003). The company does not exist today. In 2000 Microsoft launched webservices as SaaS offering, followed in 2001 by IBM with their Autonomic Computing Manifesto (Kephart and Chess, 2003, IBM, 2001) and in 2007 collaboration between IBM and Google launched research in cloud computing (Lohr, 2007).

2.2.1 Definition: Cloud Computing

As the previous section has shown how cloud computing has borrowed terms and concepts from other computing paradigms, the definition of cloud computing is also "cloudy" as it has been defined differently by different industry experts and researchers alike. Larry Ellison founder of Oracle says "*we've defined cloud computing to include everything that we already do... I don't understand what we would do differently in the light of cloud computing other than change the wording of some of ours ads"* (Farber, 2008). Richard Stallman founder of the Free Software Foundation and creator of the operating system GNU says "*it's stupidity. It's worse than stupidity: it's a marketing hype campaign"* (Johnson, 2008). These comments are representative of how different experts look at cloud computing. Figure 2-1 shows the different contributors and perspective of cloud computing paradigm.

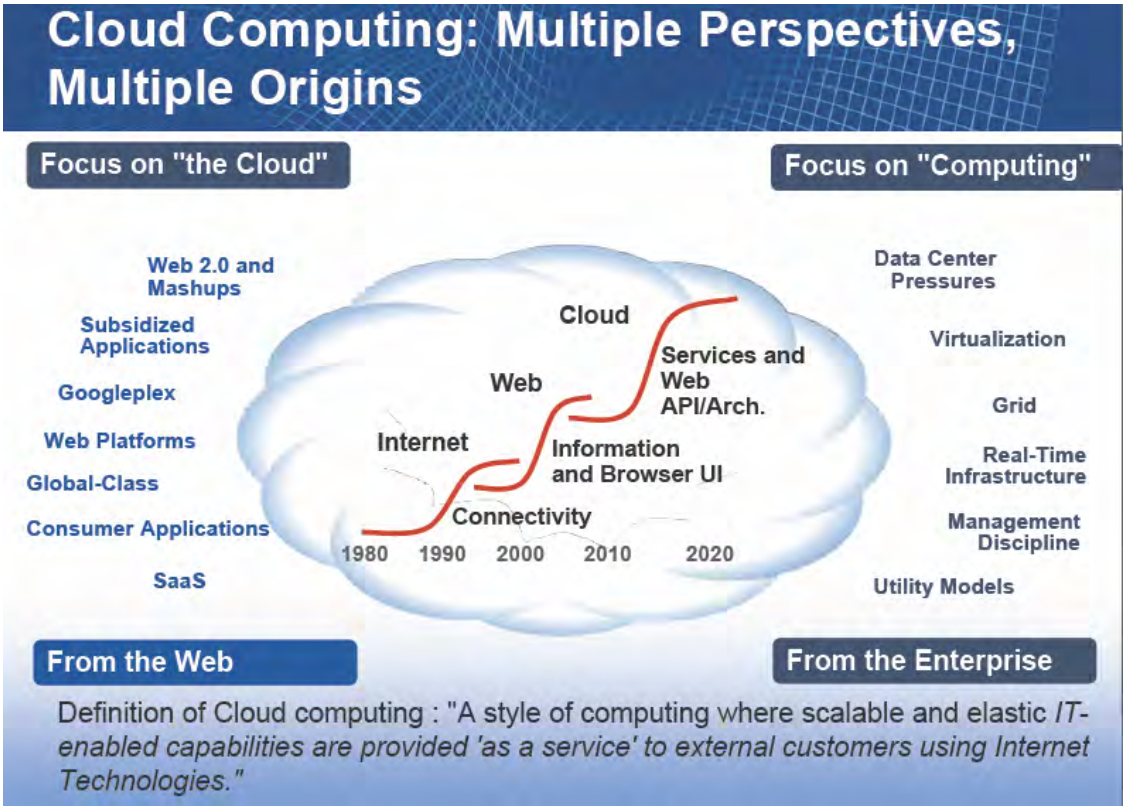

Figure 2.1: Multiple perspectives on cloud computing (Prentice, 2010)

The Gartner consulting propose a definition as follows "*A style of computing where scalable and elastic IT-related capabilities are provided as-a-service using Internet technologies to multiple external customers"* (Plummer et al., 2009). The National Institute of Standards

and Technology (NIST) defines cloud computing as " *a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., network, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics and three service models and four deployment models"* (Mell and Grance, 2009b, Mell and Grance, 2009a). Figure 2-2 shows the framework of the NIST definition of cloud computing.

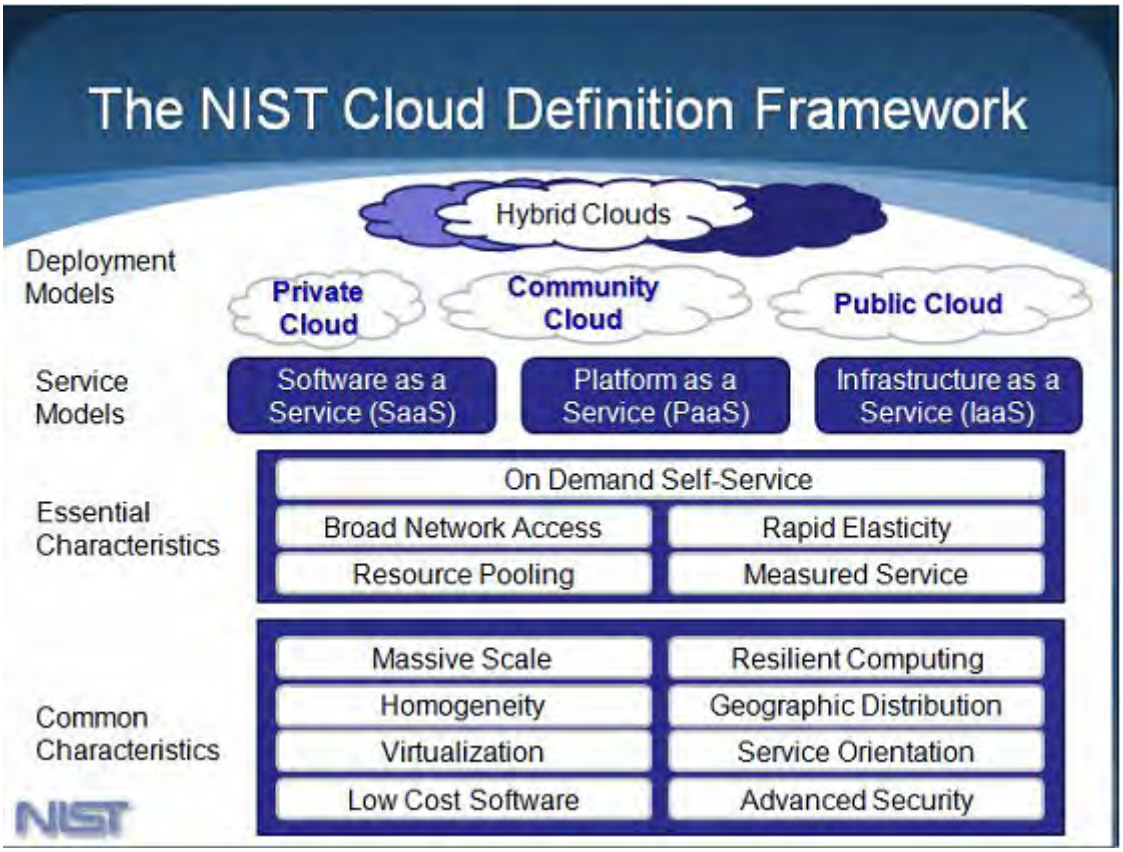

Figure 2.2: Cloud Computing Definition (Grance, 2010)

The European Network and Information Security Agency (ENISA) has defined cloud computing as "*on-demand service model for IT provision, often based on virtualisation and distributed computing technologies"* (Catteddu and Hogben, 2009). However the first academic definition of cloud computing was offered by Ramnath Chellapa in 1997 where he defined the term cloud as "*a computing paradigm where the boundaries of computing will be determined rationale rather than technical"* (Chellapa, 1997).

Other common academic and scholarly definitions are as follows: according to (Buyya et al., 2008) cloud computing is "*a type of parallel and distributed system consisting of collection of interconnected and virtualised computers that are dynamically provisioned and present as on or more unified computing resource based on service-level agreements established through negotiation between service provider and customer"*. Another common academic definition defines cloud computing as *"a set of network enabled services, providing scalable, QoS guaranteed, normally personalised, inexpensive computing platforms on demand, which could be accessed in a simple and pervasive way"* (Wang and Laszewski, 2008), while Luis et, al,.(2009) proposes the following definition " cloud are *a large pool of easily usable and accessible virtualised resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust a variable load (scale), allowing also for an optimum resource utilisation. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure provider by means of customised SLAs"*. These different definitions shows the varied understanding of what cloud computing is from the different perspectives of different stakeholders such as; academicians, architects, consumers, developers, engineers and managers (CSA, 2009). Table 2-1 provides and except of cloud definitions that are currently available as summarised by Luis et, al.,(2009) and adapted by the author.

Author/Rreference	**Year**	**Definition/Excerpt**
M. Klems (Geelan, 2009)	2008	*"you can scale your infrastructure on demand within minutes or even seconds, instead of days or weeks, thereby avoiding under-utilisation(idle servers) and over utilisation (blue screen)of in-house resources".*
P. Gaw (Geelan, 2009)	2008	"*refers to the bigger picture...basically the broad concept of using the internet to allow people to access technology enabled services".*
R. Buyya (Buyya et al., 2008)	2008	"*a type of parallel and distributed system consisting of collection of interconnected and virtualised computers that are dynamically provisioned and present as on or more unified computing resource based on service-level agreements established through negotiation between service provider and customer".*
R. Cohen (Geelan, 2009)	2008	"*for me the simplest explanation for cloud computing is describing it as, 'internet centric software'. This new cloud computing software model is a shift from traditional single tenant approach to software development to that of scalable, multi-tenant, multi-platform, multi-network, and global".*
J. Kaplan (Geelan, 2009)	2008	" *a broad array of web-based services aimed at allowing users to obtain a wide range of functional capabilities on a 'pay-as-you-go' basis that previously required tremendous hardware/software investment and professional skills to acquire".*
D. Gourlay (Geelan, 2009)	2008	"*cloud will be the next transformation over the next several years, building off of the software models that virtualisation enabled"*
D. Edwards (Geelan, 2009)	2008	"*...what is possible when you leverage web scale infrastructure (application and physical)in an on-demand way. ...anything as a service... all terms that couldn't get it done. Call it 'cloud' and everyone goes bonkers".*
B. De Haff (Geelan, 2009)	2008	"...there are really only three types of services that are cloud based: SaaS, PaaS, and Cloud Computing Platforms".
B. Keppes (Geelan, 2009)	2008	"*put cloud computing is the infrastructural paradigm shift that enables the ascension of SaaS".*
K. Sheynkman (Geelan, 2009)	2008	"*the 'cloud' model initially focused on making hardware layer consumable as on-demand compute and storage capacity. ... to harness the power of the cloud, complete*

		application infrastructure needs to be easily configured, deployed, dynamically scaled and managed in these virtualised hardware environments".
O.Sultan (Geelan, 2009)	2008	"*... in a fully implemented Data center 3.0 environment, you can decide if an app is run locally (cook at home), in someone else's data center (take-out) and you can change your mind on the fly in case you are short on data center resources (pantry is empty) or you having environmental/facilities issues (too hot to cook)".*
K.Harting (Geelan, 2009)	2008	"*cloud computing overlaps some of the concepts of distributed, grid and utility computing, however it does have its own meaning if contextually used correctly. Cloud computing really id accessing resources and services needed to perform functions with dynamically changing needs".*
J. Pritzker (Geelan, 2009)	2008	"*cloud tend to be priced like utilities... i think is a trend not a requirement".*
T. Doerksen (Geelan, 2009)	2008	"*cloud computing is... the user friendly version of grid computing".*
T. von Eicken (Geelan, 2009)	2008	"*... outsourced, pay-as-you-go, on-demand, somewhere in the internet".*
M. Sheedan (Geelan, 2009)	2008	"*... 'cloud pyramid' to help differentiate the various cloud offerings out there... top: SaaS; middle: PaaS; bottom: IaaS".*
A. Ricadela (Geelan, 2009)	2008	*"... cloud computing projects are more powerful and crash proof than Grid systems developed even in recent years*"
I. Wladawsky Berger (Geelan, 2009)	2008	*"... the key thing we want to virtualise or hide from the user is complexity. ...with cloud computing our expectation is that all that software will be virtualised or hidden from us and taken care of by systems and /or professionals that are somewhere else – out there in the cloud".*
B. Martin (Geelan, 2009)	2008	"*cloud computing really comes into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software"*
R. Bragg (Bragg, 2008)	2008	" *the key concept behind the Cloud is Web application... a more developed and reliable Cloud".*
G. Gruman and E. Knorr	2008	"*cloud is all about: SaaS... utility computing... Web services... PaaS... Internet integration... commerce platforms...".*
P. McFedries (McFedries, 2008)	2008	"*cloud computing, in which not just our data but even our software resides within the cloud, and we access everything not only thorugh our PCs but also cloud-friendly devices, such as smartphones, PDAs... the megacomputer enabled by virtualisation and software as a service... this is utility computing powered by massive utility data center".*
Gartner(Plummer et al., 2009)		"*A style of computing where scalable and elastic IT-related capabilities are provided as-a-service using Internet technologies to multiple external customers*

Table 2.1: Cloud definitions Adapted from Luis et, al., (2009)

After a thorough review of existing cloud computing definitions and the computing paradigms from which cloud computing borrows terms and concepts, in this dissertation we define cloud computing as a new computing paradigm, that involves the outsourcing of data and/or computing resources with capabilities for expandable resource scalability, on-demand provisioning of computing resources with little or no upfront costs. However, organisational and institutional need for better value for money from their IT investments is the key factor driving cloud computing. The following sub-section highlights the essential and common characteristics of cloud computing paradigm.

2.2.2 Characteristics

Cloud computing has a number of characteristics that distinguishes it from other computing paradigms. These characteristics can be categorised as essential characteristics and common characteristic. The NIST has identified five essential characteristics (Plummer et al., 2009)

and eight common characteristics of cloud computing (Grance, 2010, Mell and Grance, 2009a).The essential characteristics are:

On Demand Self-Service: allows for provisioning of computing resources automatically as needed.

Broad Network Access: access to cloud resources is over the network using standard mechanisms provided through thin or thick clients in a heterogeneous manner. For example through Smartphone's, mobile phones and laptop computers.

Resource Pooling: the vendors' resources are capable of being pooled to serve multiple clients using a multi-tenant model, with different physical and virtual resources in a dynamic way. The pooling and assigning of resources is done based on the changing needs of clients or consumers. Example of resources include; computation capabilities, storage and memory.

Rapid Elasticity: allows for rapid capability provisioning, for quick scaling out and scaling in of capabilities. The capability available for provisioning to the client seems to be unlimited and that it can be purchased as demanded.

Measured Service: allows monitoring, control and reporting of usage. It also alows for transparent between the provider and the client.

In conjunction with the essential characteristics as identified by NIST, there are other cloud computing characteristics (GNi, 2009, Miller, 2008, Luis et al., 2008, Vouk, 2008, Grance, 2010). These characteristics are such as: massive scale availability of computing and storage capabilities, homogeneity, use of virtualisation technology, resilient computing, and pay-as-you go model. Low or no up-front IT infrastructure costs, geographical distribution of clouds, low overhead costs for IT and administration personnel.

These characteristics make cloud computing attractive to business organisations and government agencies. The next sub-section looks on the different technologies that underlies cloud computing.

2.2.3 Technology

In this sub section cloud computing is reviewed from a technology point of view. The industry has already defined the technology in various ways. Improvement in technology

and in particular virtualisation have contributed greatly in the advent of cloud computing. Other technology that have had impact on the rise of cloud computing include utility computing, grid computing, parallel computing and service oriented architecture (Mell and Grance, 2009b, Luis et al., 2008, Vouk, 2008, Wang and Laszewski, 2008), thus cloud computing is combination of many different technologies.

The technologies that underpin the advent of cloud computing are: *grid computing*, virtualisation, parallel computing, service oriented architecture (SOA), the Internet, autonomic system computing, Web services, web application frameworks and open source software. There are also business models that have paved the way for cloud computing. These are Web 2.0, Software as a Service, utility computing, service level agreements, open standards, data portability and accessibility (Mell and Grance, 2009b). These technologies and business models prepared the platform for cloud computing for offering such capabilities such as: the representation of computation, storage as logical entities through virtualisation (Bhattacharjee, 2009, Vouk, 2008); this enables the creation of multiple instances of the virtual machines based on the physical machine or storage for use by multiple users (Buyya et al., 2008, Wang and Laszewski, 2008). Service oriented achirtecture and web services enables offering of cloud computing services as web services accessible via the Internet, also SOA makes it possible for cloud services to be available in multiple platforms (Wang and Laszewski, 2008); grid computing offered to cloud the capabilities for resource sharing, heterogeneity and ability to de-centralise resource control (Luis et al., 2008). Since cloud computing services are web application or web based application accessed via the Internet, Web 2.0 provides cloud computing with capabilities of improved connectivity and interaction between web applications. This makes access to cloud computing services by users more efficient and easy (Wang and Laszewski, 2008)

These technologies are the key technologies underpinning the evolution and success of cloud computing. This is because these technologies paved the way for the platform from which cloud computing is launched. They provided the technology and infrastructure that cloud computing relies on. They also provided the theoretical and practical experiences which cloud computing capitalises on for its success and adoption in business organisations. The next subsection describes the delivery and deployment models used in cloud computing in offering its services.

2.2.4 Service/Delivery and Deployment Models

Cloud computing has three delivery or service models and four deployment models that are popular (Vouk, 2008, CSA, 2009, Mell and Grance, 2009a, Mell and Grance, 2009b). These models are describe briefly in this section as follows:

Service/delivery models

There are three common service models for offering cloud computing services. These models are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) (CSA, 2009). In SaaS the organisation outsources everything by renting remotely accessed services via the Internet. The client uses the provider's applications or software through different client devices via a thin client interface such as a web browser (CSA, 2009). However, in this delivery model the client does not have control or manage the infrastructure through which the applications are running (CSA, 2009, Mell and Grance, 2009a). Examples of SaaS providers are salesforce.com, Netsuite and Oracle CRM on Demand. For PaaS, the service provider rents dedicated resources to a client. In this offering the client has the ability to deploy on the cloud his/her own created applications or software using programming languages and tools supported by the provider. This model offers some contol to the user which is related to the deployed applications but not to the cloud infrastructure (CSA, 2009, Mell and Grance, 2009a). Examples of Paas services are Google Application Engine, force.com and cloud 9 Analytics.

The third delivery model for cloud computing is Infrastructure-as-a-Service (IaaS). In this service model dedicated resources are offered to a single tenant or client and do not allow sharing of dedicated resources to unknown third parties. The model provides the customer with ability to deploy applications on the cloud infrastructure. The applications may include operating systems and other applications. However, the customer does not have control over the infrastructure but may control the deployed applications and operating systems, storage and selected network components (Mell and Grance, 2009a). Figure 2-3 shows the cloud taxonomy showing different types of offerings in the different delivery models.

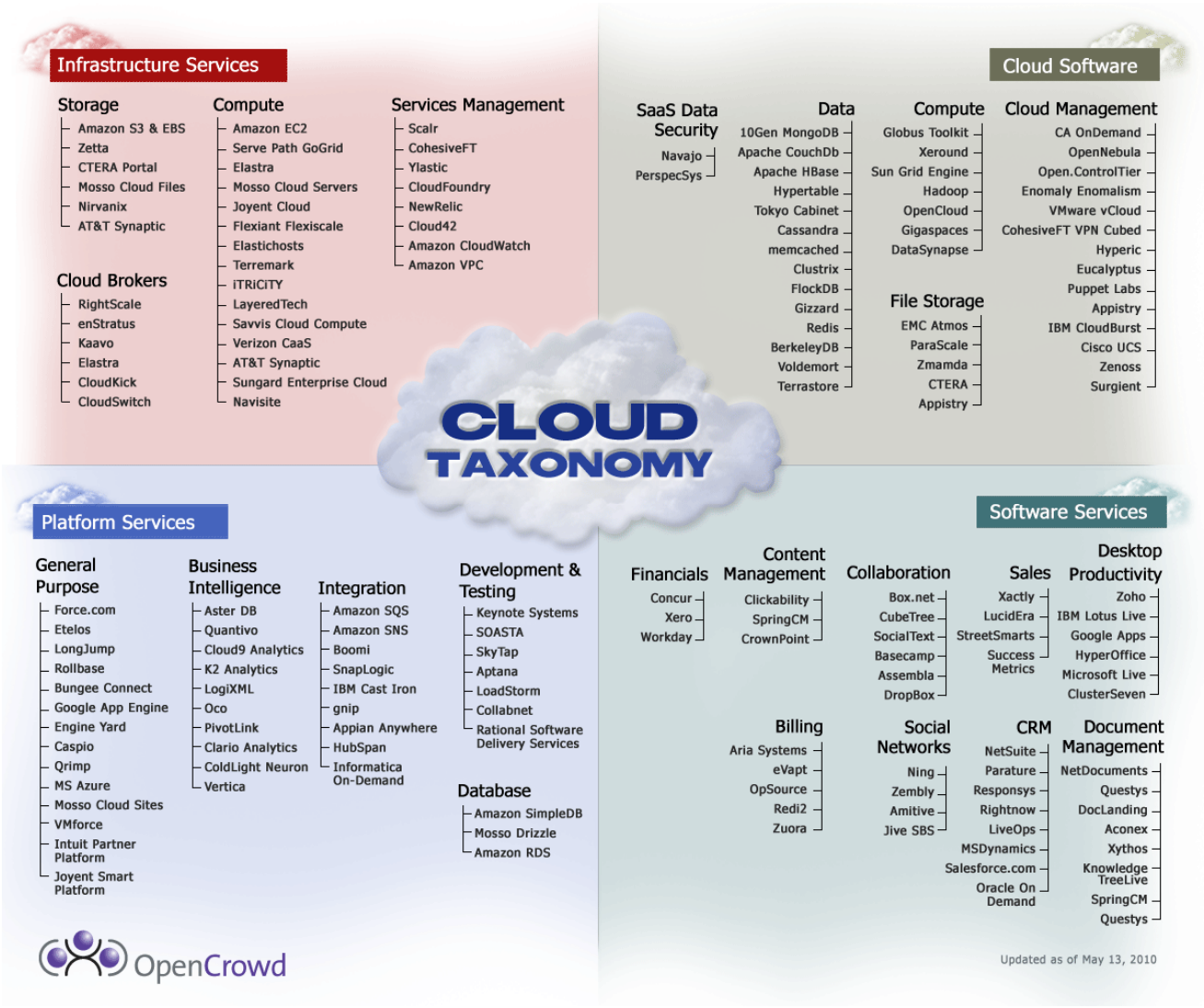

Figure 2.3: Cloud Taxonomy (OpenCrowd, 2010)

Deployment models

There are four models for cloud computing service deployment, regardless of the service or delivery model (IaaS, PaaS, or SaaS) adopted. These deployment models may have different derivatives which may address different specific needs or situations (Dustin Amrhein et al., 2010, CSA, 2009). The basic deployment models are public cloud, private cloud, community cloud and hybrid cloud(CSA, 2009, Dustin Amrhein et al., 2010, Grance, 2010, Mell and Grance, 2009a, Catteddu and Hogben, 2009).

Public cloud in this deployment the cloud infrastructure is accessible to general public and shared in a pay as you go model of payment. The cloud resources are accessible via the internet and the provider is responsible for ensuring the economies of scale and the management of the shared infrastructure. In this model clients can choose security level they need, and negotiate for service levels (SLA). The first and most used type of this offering is the Amazon Web Services EC2. Figure 2-4 show the structural formation of a public cloud.

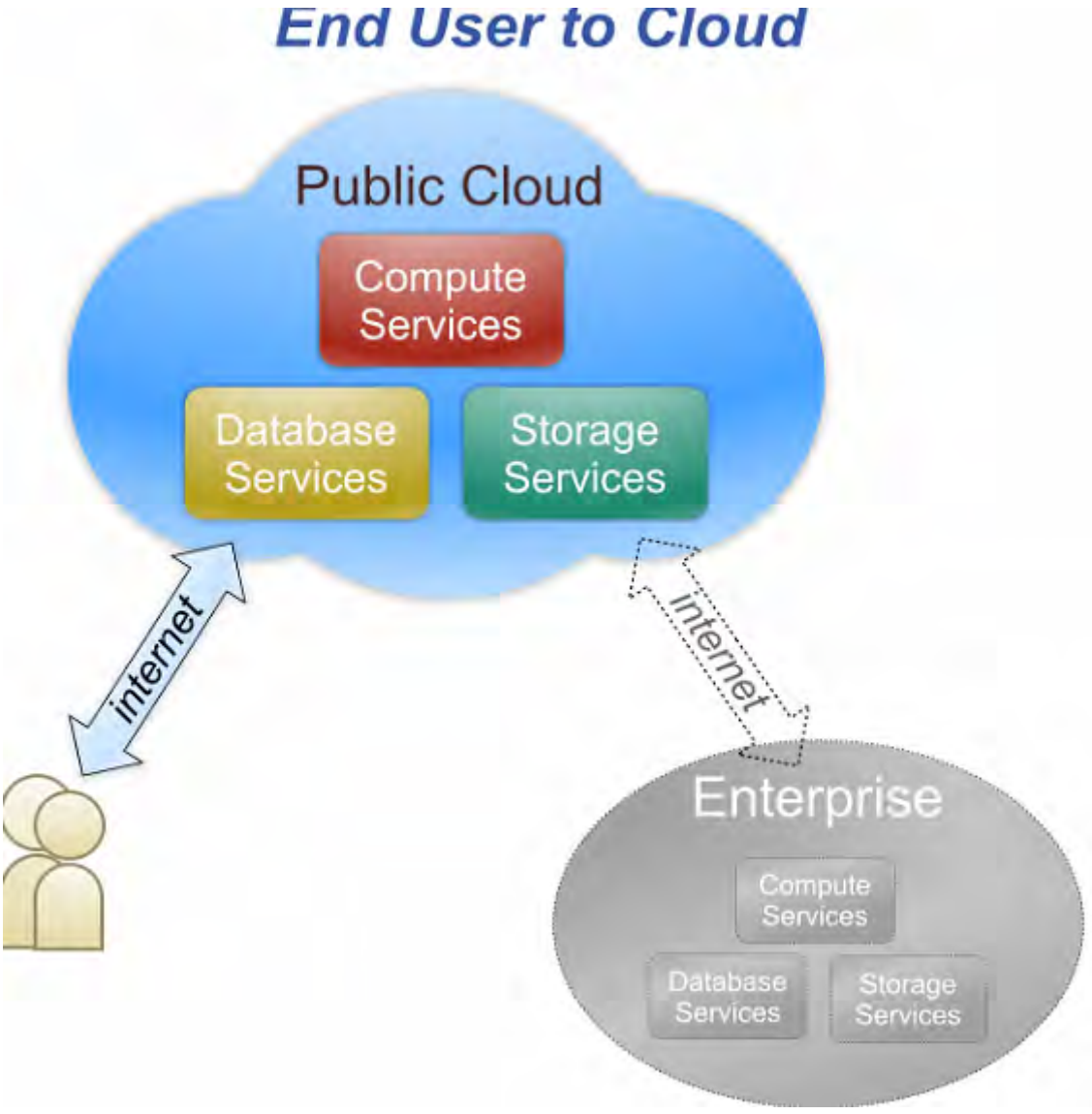

Figure 2.4: Public Cloud (Dustin Amrhein et al., 2010)

In this type of cloud, the organisation does not access or use the public cloud which is accessible to the general public.

Private cloud is another deployment model for cloud services. In this model the cloud resources are not shared by unknown third parties. The cloud resources in this model may be located within the client organisation premises or offsite. In this model the clients security and compliance requirements are not affected though this offering does not bring the benefits associated with reduced capital expenditure in IT infrastructure investments. Figure 2-5 shows the structural formation of a private cloud.

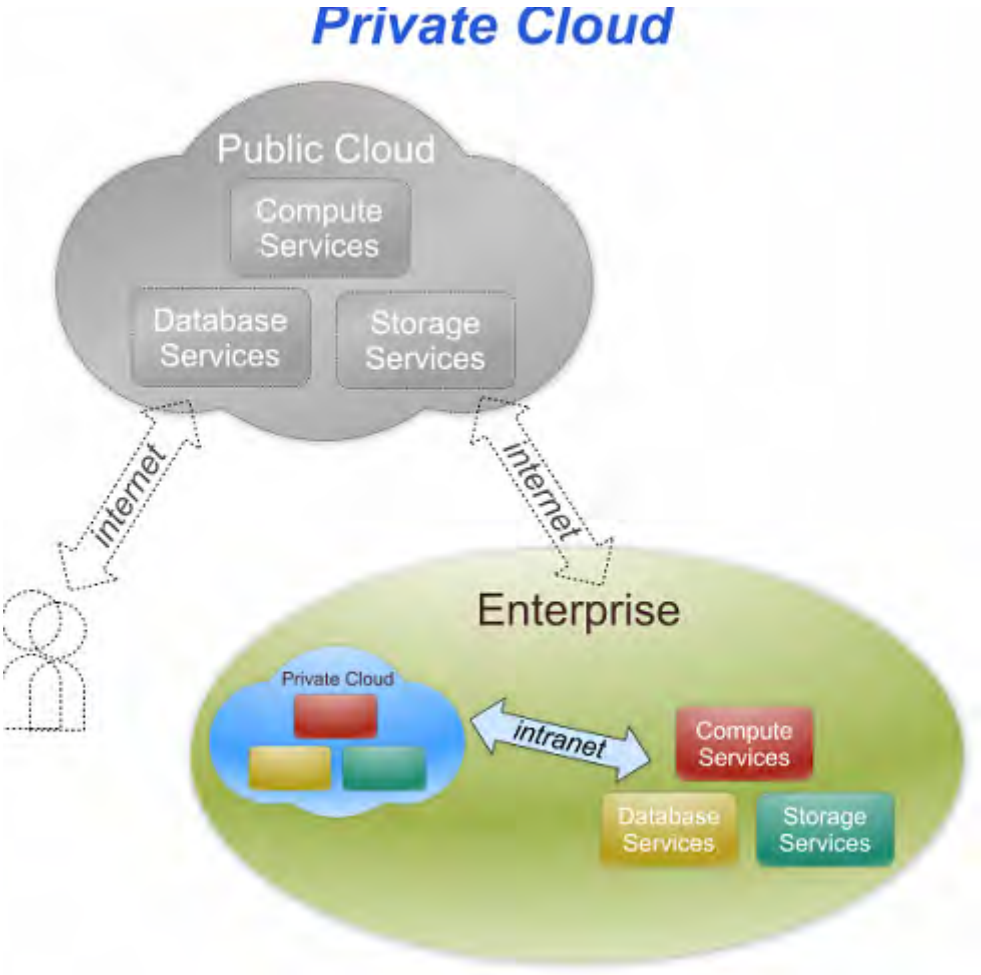

Figure 2.5: Private Cloud (Dustin Amrhein et al., 2010)

In this type of cloud the general public does not have access to the private cloud neither does the organisation use the public cloud.

Hybrid cloud as its name implies is a model of deployment which combines different clouds for example the private and public clouds. In this model the combined clouds retains their identities but are bound together "*by standardised or proprietary technology*" (CSA, 2009). Figure 2-6 shows the hybrid cloud formation

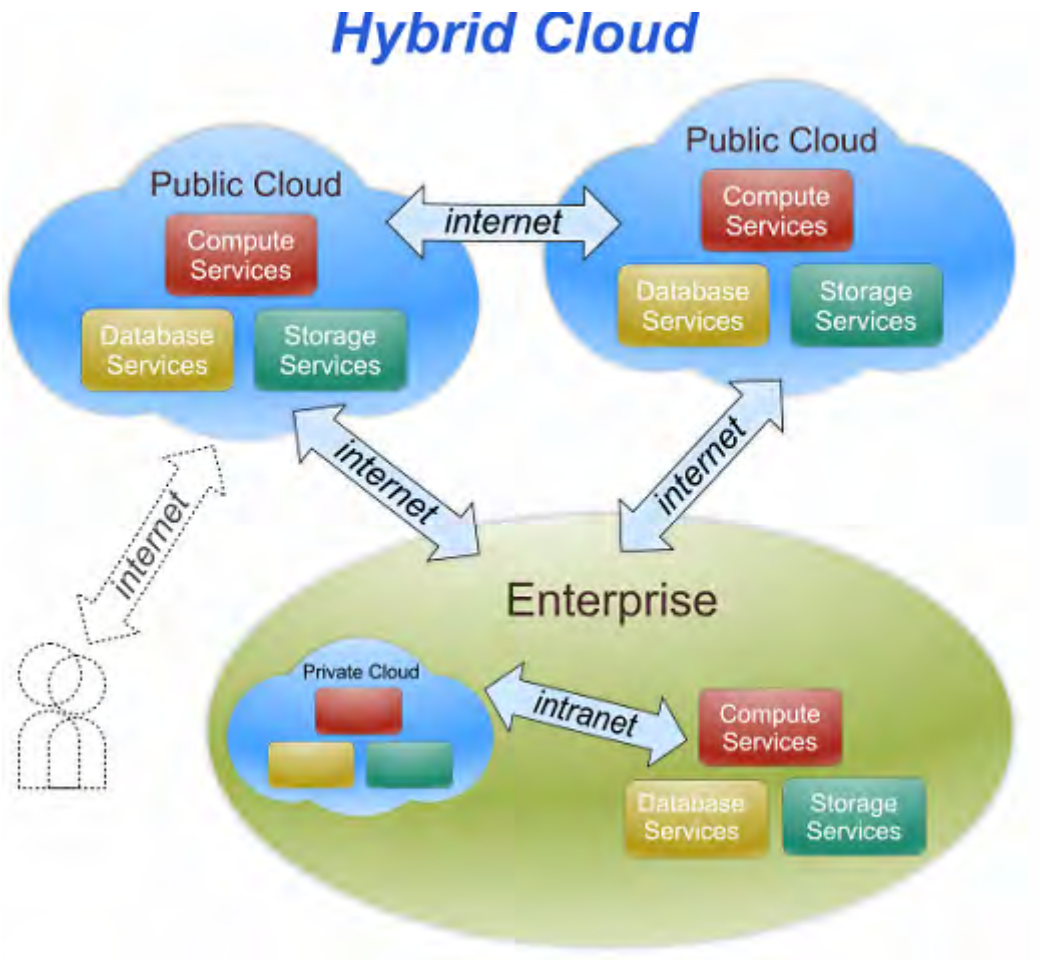

Figure 2.6: Hybrid Cloud (Dustin Amrhein et al., 2010)

In this type of cloud the general public does not have access to the cloud, but the organisation uses infrastructure in both the public and private cloud.

Community cloud is the fourth deployment model that can be used to deliver cloud computing services. In this model the cloud infrastructure is shared by multiple organisations or institutions that have a shared concern or interest such as compliance considerations, security requirements. This type of cloud may be managed by the organisation or by a third party and may be located on-premises or off-premises. Figure 2-7 shows the community cloud.

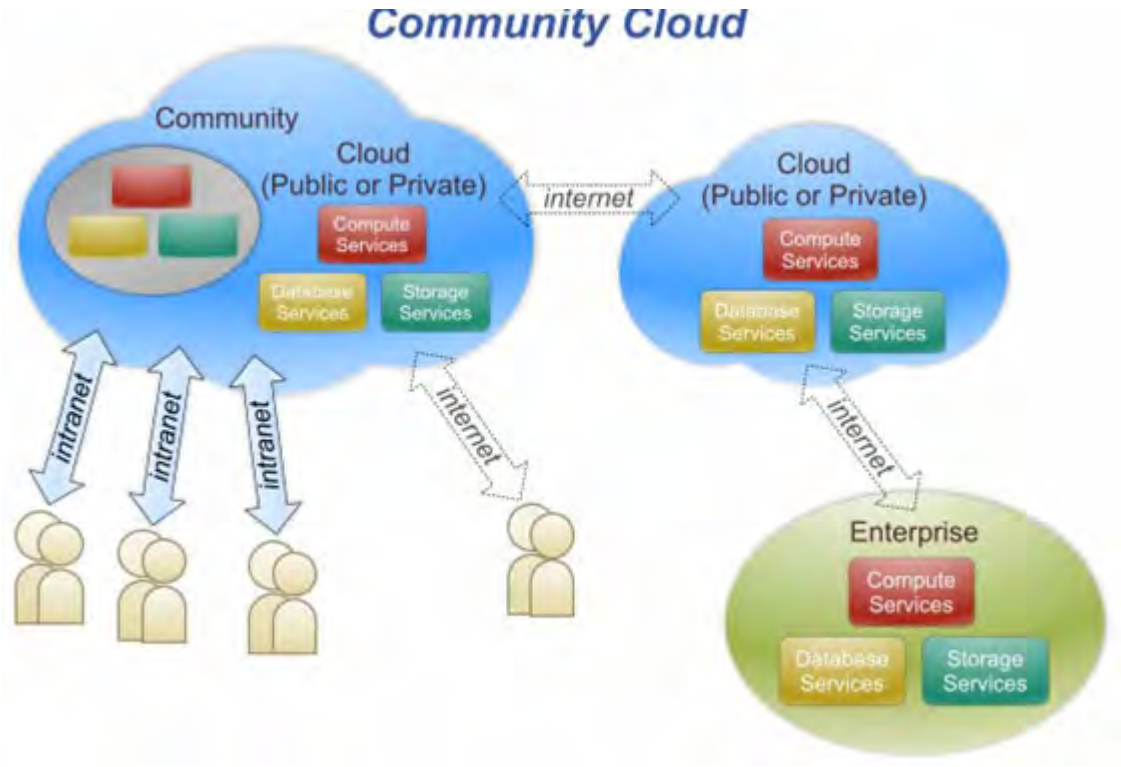

Figure 2.7: Community Cloud (Dustin Amrhein et al., 2010)

In this type of cloud both the public and the organisations forming the community cloud have access to the cloud services offered by the community cloud.

2.2.5 Drivers for adoption and benefits of cloud computing

Cloud computing with its different deployment and delivery models offers a number of benefits to businesses (Voona and Venkantaratna, 2009, Buyya et al., 2008, Miller, 2008, Catteddu and Hogben, 2009, Andrei, 2009). These benefits are such as: economies of scale resulting in low-costs of IT infrastructure, low maintenance costs and low IT administration costs. Other benefits are, improved of performance as a result of having access to dynamic and scalable computing, memory and storage capabilities based on demand. Cloud computing also offers easier data monitoring, quick incident response, and low costs to undertake security measures. Easier group collaboration, universal access to computing resources and the removal for the need for specific devices or hardware in-house are also benefits that can be accrued from cloud computing.

However, cloud computing has a number of disadvantages such as: requiring a constant internet connection, can be slow in case of slow internet connections, limited features offering, security might not meet the organisation standards, danger of loss of business in case of data loss or cloud vendor filing for bankruptcy (Miller, 2008, Jeffrey and Neidecker-Lutz, 2009, Ristenpart et al., 2009).

Figure 2-8 shows a summarised view of the cloud computing system, highlighting its stakeholders, locality of hosting, modes of delivery, types of cloud offering, its features, and benefits.

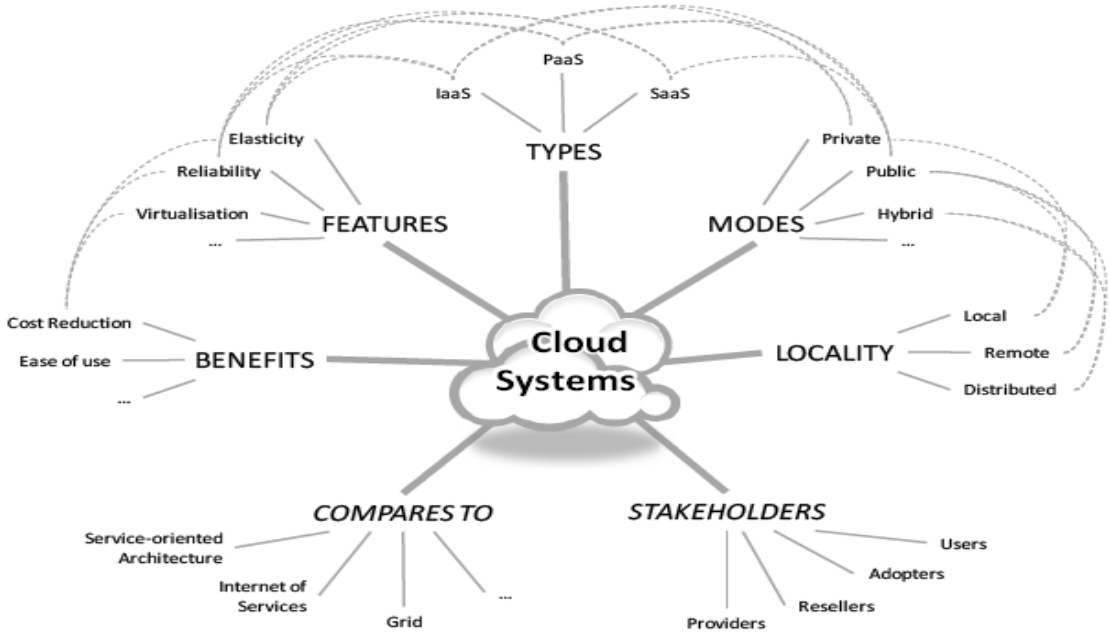

Figure 2.8: The Cloud computing systems (Jeffrey and Neidecker-Lutz, 2009)

However, in order to understand the different challenges and trust risks associated with cloud computing, *"understanding the relationships and dependencies between these delivery models (IaaS, PaaS & SaaS) is critical*" (CSA, 2009). This is because cloud computing offerings build upon each other. IaaS being the foundation on which the other two build on. PaaS build on top of IaaS while SaaS build on top of PaaS. This means that each layer that build upon the layer below it inherits the strengths as well as weaknesses of that layer, as well as the security issues and risks (CSA, 2009). The Cloud Security Alliance's cloud reference model highlights the need for understanding these relationships and dependencies as shown in figure 2-9.

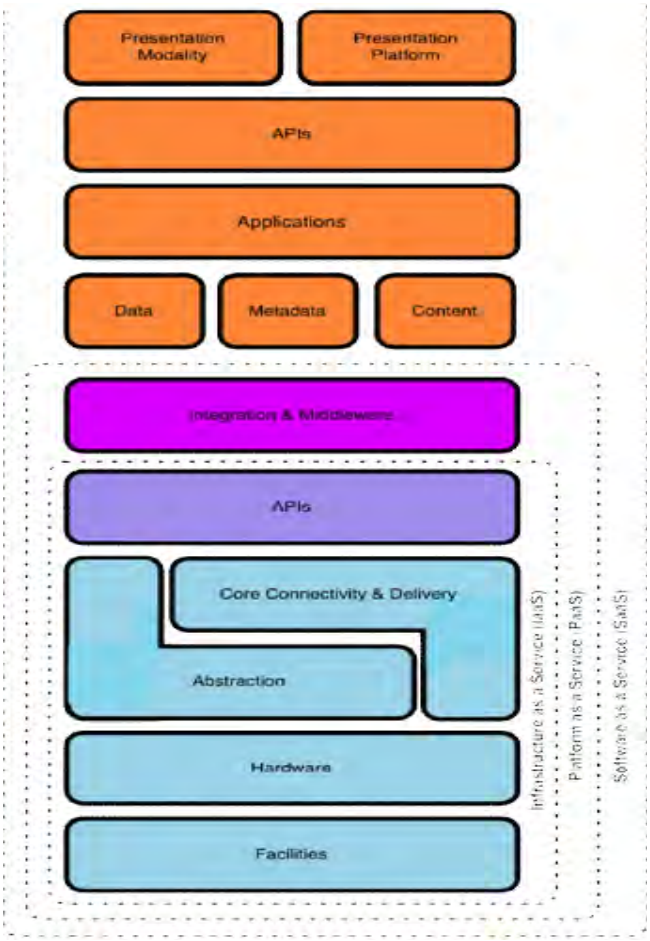

Figure 2.9: Cloud Reference Model (CSA, 2009)

2.3 Conclusion

This chapter has reviewed cloud computing providing its definition, characteristics, and drivers for its adoption. Chapter 3 discusses trust issues in computer science and particular in cloud computing.

3. TRUST IN COMPUTER SCIENCE

3.1 Trust in Computer systems

As introduced in section 1.3 and 2.1, trust is linked to all challenges facing cloud computing adoption. However, trust is greatly affected by security of information and It systems is in jeopardy. John Chambers Chairman and CEO of CISCO Systems says *"cloud computing is a security nightmare and it can't be handled in traditional ways"* (Greene, 2009). This statement echoes the "*feelings and reality of security*" (Schneir, 2008). The complexity of cloud computing makes the issue of security of paramount importance to potential clients and service providers alike. How customers feel about the security of their data and applications is affected by the vulnerabilities and potential attacks that the cloud is open to (section 4.2.1 and 4.2.2), the reality of how secure the cloud environment is posses another challenge. These two, that is the feeling and reality of security together, raises the issue of trust in using cloud computing services (section 3.3.2, 4.2, 4.3, 5.1 and 5.3).

The level of trust is dependent on how the cloud service provider appeals to the feelings of the potential client and how the reality of security risks and other challenges of cloud adoption (chapter 4 and 5) have been addressed to appeal to the customer desires and expectations. This means that, adopters of cloud services will subscribe to providers whom they deem trustworthy. In this subsection trust is defined, it qualities identified and different models of computer systems trust are identified.

3.1 Definition: Trust

"*Trust is a judgement of unquestionable utility – as humans we use it every day of our lives. However, trust has suffered a from an imperfect understanding, a plethora of definitions, and informal use in literature and in everyday life"* (Marsh, 1994). As Marsh (1994) argues, a survey of literature posses challenge and can be very confusing because of the different meanings that are attached to the term trust and the different research avenues where trust is being used (Rosseau et al., 1998, McKnight et al., 1998). In this section a brief survey of trust definition is done.

(Gambetta, 2000) defines trust as "*the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends"*. A similar definition is offered by the International Telecommunication Union (ITU) in ITU-T X.509, section 3.3.54 which defines trust as "*generally an entity is said to 'trust' a second entity when the first entity makes assumptions that the second entity will behave exactly as the first entity expects"* (ITU, 2005). These two definitions attach to trust the connotation of dependence on the trusted part and the reliability to be trusted on the trusted part by the trusting party (Audun et al., 2007). However, the complexity of trust shows that reliability alone is not enough to guarantee trust by entering into state of dependency (Audun et al., 2007, Castelfranchi and Falcone, 2002). Castlefranchi and Falcone (2002) argues that "*it is possible that the value of the danger per se (in case of failure) is too high to choose a given decision branch, and this independently either from probability of the failure (even if it is very low) or from the possible pay off (even if it is very high). In other words, that danger might seem to the agent an intolerable risk"*.

Another definition is that given by (McKnight and Chervany, 2001). They define trust as "*the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible"*. This definition carries with it the notion of rational decision making in deciding to trust a third party. Commenting on the definition Audun, et, al; (2007) says "*it explicitly and implicitly includes aspects of broad notion of trust which are 'dependence' on trusted entity or party, the 'reliability' of the trusted entity or party, 'utility' in the sense that positive utility will result from positive outcome, and negative utility will result from negative outcomes, and finally a certain risk attitude in the sense that trusting is willing to accept situational risks resulting from the previous elements"*. Marsh (1994) defines trust as "*choosing to put ourselves in another's hands, in that the behaviour of the other determines what we get out of a situation"*. Table 3-1 provides a summary of excerpts of different definitions of trust from different authors.

Author/Reference	*Definition/excerpt*
(Mui et al., 2002)	*... a subjective expectation an agent has about another's future behaviour based on history of their encounters.*
(Grandison and Sloman, 2000)	*The firm belief in the competence of an entity to act dependably, securely and reliably within specified context.*
(Olmedilla et al., 2005)	*Trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context in relation to service X.*

(Zand, 1972)	*A behaviour.*
(Cohen, 1966)	*A confidence.*
(Rotter, 1980, Scanzoni, 1979)	*An expectancy.*
(Barber, 1986, Bromiley and Cummings, 1995)	*A belief or set of belief.*
(Rotter, 1980)	*A dispositional variable.*
(Johnson-George and Swap, 1982)	*A situational variable.*
(Lewis and Weigert, 1985a, Lewis and Weigert, 1985b, Fox, 1976)	*A structural variable.*
(Shapiro, 1987)	*A social agency relationship variable.*
(Rempel et al., 1985)	*An interpersonal variable.*
(Artz and Gil, 2007)	*Refers to mechanisms to verify that the source of information is really who the source claims to be.*

Table 3.1: Definitions of Trust (source: Author, based on (McKnight et al., 1998))

A review of these different definitions shows that trust is not intended by itself to guarantee the law or insurance remedies in case of things not going according to plan, yet it does not rule out such arrangements (Audun et al., 2007).

A review of these definitions and the nature of cloud computing, lead to a conclusion on the concept of trust which reveal trust as the willingness of the client to depend on the service provider with a feeling of security given that the service provider has transparently disclosed the potential risks and mitigation plans that are used to secure the cloud.

3.2 Situations that demands trust in cloud computing

In order to build trust in cloud computing adoption, there is a need to address the different situations or instances where trust is needed. This is because according to Grandison and Sloman (2000) "*a trust decision is based on many things such as the trustor's propensity to trust, its belief and past experience relating to the trustee*". These different instances show what clients expect from the service provider before they can make a decision to subscriber for the service. Therefore, the degree of trust requirement to which each individual client attaches to the different situations may differ but nevertheless, these different scenarios are an indispensable part in building a trust relationship in cloud computing adoption. In this dissertation the classification of trust developed by Grandison and Sloman (2000) is adopted, in which identify five scenarios or situations where trust is needed in cloud computing. These scenarios are described as follows:

The first scenario is related to **access to resources or access to a trustor's resource** (Grandison and Sloman, 2000). In this scenario trust is for the purpose of accessing resources owned or under the responsibility of the trusting part (Audun et al., 2007). That is, a trustor trusts a trustee to use their resources, which may be an execution environment or an application (Abrams and Joyce, 1995). In this case trust is linked to the issues of access control which is a central theme in computer security (Abrams and Joyce, 1995, Grandison and Sloman, 2000, Audun et al., 2007). Therefore, trust is the basis for forming authorisation policies (Grandison and Sloman, 2000). In cloud computing building trust is crucial given the nature of cloud computing environment. The need to prove that cloud service provider can be trusted in issues such as, escalated privileges and possibilities of insider attacks (Santos et al., 2009) is of paramount importance. This is because without such proof, trust cannot be established between the provider and the client. Example of resource access trust in cloud computing are such as the client trusts the service provider's administrators to manage their resources hosted in the providers cloud infrastructure.

Service provision is another scenario. Grandison and Sloman (2000) calls it provision of service by the trustee, while Audun et, al (2007) call it provision trust. It is also known as business trust by the Liberty Alliance Project (Boeyen et al., 2003). In this case, the client places their trust on the service provider. This service provision does not involve access to the trustor's resources (Boeyen et al., 2003, Grandison and Sloman, 2000). However, this may not be true of cloud computing. This is because data and or application may be residing in the service provider's infrastructure which may mandate the access by service provider's administrators for optimum performance of the infrastructure. In cloud computing environment, this trust relates to the needs of client to be shielded from perceived threats and/or attacks. For this to be evident in cloud computing, service providers need to have well formed and prepared Service level agreements (SLAs) with clients and other types of contracts that are of concern to clients. This scenario demands that, the client must trust the computing environment provided by the cloud computing.

Certification of trustees (Grandison and Sloman, 2000), or identity trust (Audun et al., 2007) or authentication trust (Boeyen et al., 2003) is another case where trust is need in cloud computing. This is a scenario which requires the client to believe that the service provider is as it claims to be. It is based on certification by third party of the trustworthiness

of the trustee (Grandison and Sloman, 2000). There are different systems that derive trust based on identity (Audun et al., 2007) such as PGP and X.509 (ITU, 2005). With lack of certification and standards governing cloud computing environment, this type of trust is not easily achieved. Thus, cloud service providers need to assure clients about the type of service they offer, and that they can deliver what they promise and that, they are who they claim to be.

Delegation trust occurs when the client trusts the service provider to act on their behalf. The service provider makes decisions on behalf of the client on resources that the client owns or controls (Grandison and Sloman, 2000). In cloud computing this may mean that the service provider performs security audit, e-discovery among other things on behalf of the client. Grandison and Sloman (2000) see this type of trust as "*a trust decision-making service*". Therefore, this calls for cloud computing service providers to develop mechanisms that will assure customers in issues such as forensic evidence gathering. Compliance issues such as, with data protection laws; and other regulations and security standards that clients are to comply with (chapter 3 and section 4.2), and they are capable to act on their behalf in accordance with such requirements.

The last scenario where cloud computing demands trust is in the case of **infrastructure trust**. This scenario describes the extent to which the trusting party believes that the necessary systems and institutions are in place in order to support transactions and provide safety net (Audun et al., 2007). This kind of trust is also known as context trust (Audun et al., 2007) and system trust (McKnight and Chervany, 1996). This trust concerns itself with the infrastructure that the trustor must trust (Grandison and Sloman, 2000). In cloud computing, vendors need to work together with customers in building this trust through collaboration in developing and setting up security policies, SLAs agreements and issues of legislation and compliance (section 4.2.4, 4.3.2, 5.5, 5.6 and 6.2).

3.3 Qualities of trust relationship

Trust as a characteristic and quality of relationship between client and vendor, need to balance between responsibility and diligence. It should aim at facilitating the confidence that something will or will not occur in a promised way. Therefore, trust is a two way relationship (Andert et al., 2002), and it has a number of characteristics and

qualities(Friedman et al., 2000, Andert et al., 2002, Pearson et al., 2005, Audun et al., 2007, Grandison and Sloman, 2000).

3.4 Models of trust

Different researches have been conducted in the area of trust in computer and information systems. In this section a categorisation of these different researches into generally four broad categories is done.

Policy-based trust

The models in this category use policies to establish trust between two entities. The focus is on managing the exchange of credentials and enforcement of access policies. The underlying assumptions behind these models is that, trust can be established by a sufficient amount of credentials supplied by an entity wishing to have access to another entity or resource. Through the obtained credentials policies are enforced to grant the requesting entity the required level of access. In these models the use of a third party for credential issuing and validation is employed. Models in this category can be classified as network security credentials (Kohl and Neuman, 1993, Neuman and Ts'o, 1994); trust negotiation (Yu et al., 2001, Yu and Winslett, 2003, Winslett et al., 2002, Lia et al., 2003, Nejdl et al., 2004); security policies and trust languages (Tonti et al., 2003, Uszok et al., 2003, Kagal et al., 2003, Nielsen and Krukow, 2003, Carbone et al., 2003, OASIS, 2005a, OASIS, 2005b, OASIS, 2007); distributed trust management (Blaze et al., 1996, Blaze et al., 1999, Thompson et al., 1999); and effect of credentials(Zheng et al., 2002, Bos et al., 2002, Riegelsberger, 2002) .

For cloud computing policy based trust models are faced with the challenge of ensuring that credentials are properly managed. This is because with the nature of cloud which is distributed system in multiple locations the more credentials are revealed the more likely is compromise to occur.

Reputation-based trust

In this category, trust is established through the use of reputation. The reputation of an entity is determined bases on past interactions or performance and used to determine or access its future behaviour. In these models trust is computed or determined by the use of an entity

actions or behaviour from past interactions. Also referral information may be used in computing trust where first hand information is lacking. In this category reputation based trust models can be classified as: decentralisation and referral trust (Abdul-Rahman and Hailes, 1998, Abdul-Rahman and Hailes, 2000, Abdul-Rahman and Hailes, 1997, Yu and Singh, 2002); trust metrics in a web of trust (Golbeck and Hendler, 2004a, Golbeck and Hendler, 2004b, Golbeck and Hendler, 2006, Golbeck, 2005, Stewart, 2003, Stewart and Zhang, 2003); trust in peer-to-peer networks and grids (Kamvar et al., 2003, Dellarocas, 2003, Alunkal, 2003, Cornelli et al., 2002, Damiani et al., 2002, Xiong and Liu, 2002, Marti and Garcia-Molina, 2006); and application specific reputation (Pirzada and McDonald, 2004a, Pirzada and McDonald, 2004b, Pirzada and McDonald, 2006, Dash et al., 2004, Foster et al., 2004, Jøsang and Ismail, 2002).

In cloud computing, reputation based trust face the challenge of determining reputation of communicating entities. This is made more complex and difficulty in case of multi-tenancy where the communicating entities may not have prior communication for which use in determining reputation.

General models of trust

This is the most researched area of trust with modelling and definitions, pre-requisites, conditions, components and consequences (Artz and Gil, 2007). Models in this category address how human and agents trust decisions are made, describe factors or values of importance in computing trust and draws mush of its concepts from psychology and sociology in determining what trust is made of. Models in this category address issues such as access control policies, specifying who to trust, beliefs, risks and utility of trust. In this category models can be classified as: general characteristics of trust (McKnight and Chervany, 1996, McKnight and Chervany, 2001, Gefen, 2002, Wang and Emurian, 2005, Acrement, 2010, Mui et al., 2002); computational and online trust (Krukow et al., 2009, Sassone et al., 2006, Krukow et al., 2008, ElSalamouny et al.); game theory and agents (Nielsen et al., 2007, Marsh, 1994, Friedman et al., 2000, Falcone and Castelfranchi, 2004, Mayer et al., 1995); and software engineering based trust (Alcalde et al., 2009, Viega et al., 2001a, Viega et al., 2001b, Grandison and Sloman, 2002).

For cloud computing the general model of trust provides a way of understanding what cloud customers may expect from vendors.

Information resources trust

These models of trust deal with the question of whether information resources such as websites are trustworthy and how to measure trust of different information resources or sources that are web-based (Artz and Gil, 2007). Information resources trust can be classified as: web resources trust (Grandison and Sloman, 2000, Dondio and Barret, 2007), hyperlink trust , and content trust

3.4.1 Cloud computing trust models

In this sub-section a number of trust models are identified and analysed to see how they respond to the issue of trust in cloud computing. The selected models are representative and do not present all the models of trust. They have been selected due to their explicit relationship to cloud computing.

Trusted Cloud Computing Platform (TCCP) (Santos et al., 2009).

This model addresses the problem of root level access to the insider. It is also addressing the problem for Infrastructure-as-a-service (IaaS) delivery model of cloud services. It assumes that there is a trusted third part that monitors the transactions in the cloud. Figure 3-1 shows the TCCP architecture.

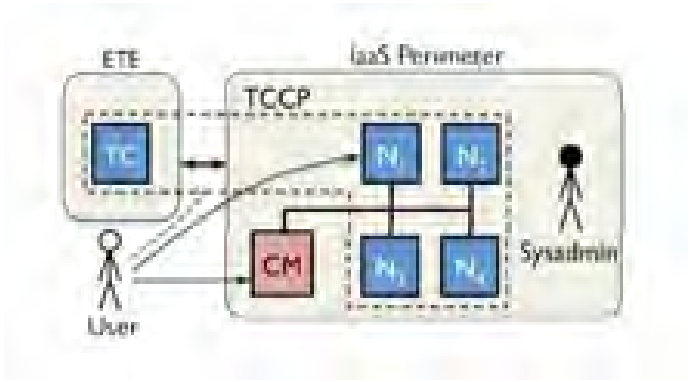

Figure 3.1: TCCP architecture (Source**:** (Santos et al., 2009).

Its limitations are, it only addresses one type of cloud computing delivery model, the IaaS, and there is a possibility of single point of failure and the possible increase in the attack surface. It also adds computation requirements and hence it may not be a cost effective way.

Private Virtual Infrastructure (Krautheim, 2009)

This model addresses the problem of transparency whereby the service provider hides the internal security details from the customer. This hiding of the details results in mistrust. In order to enable the transparency collaboration between customer and service provider a factory is used.

The aim of the model is to enable collaboration between the cloud service provider and the customer to create a trusted system, enable separation of different clients through their exclusive private virtual infrastructure and give more control to customers.

Its limitations, that it leads to management overheads both to cloud service provider and the customer; it does not address the issue of secure factory that enables the customer to manage their virtual clouds. If the factory is compromised the whole is compromised.

Cloud Cube Model (JERICHO, 2009)

This model aims at enabling secure collaboration in the clouds. It aims to achieve this by helping organisation choose the right cloud formation that best sui their business needs. Figure 3-2 shows the cloud cube model.

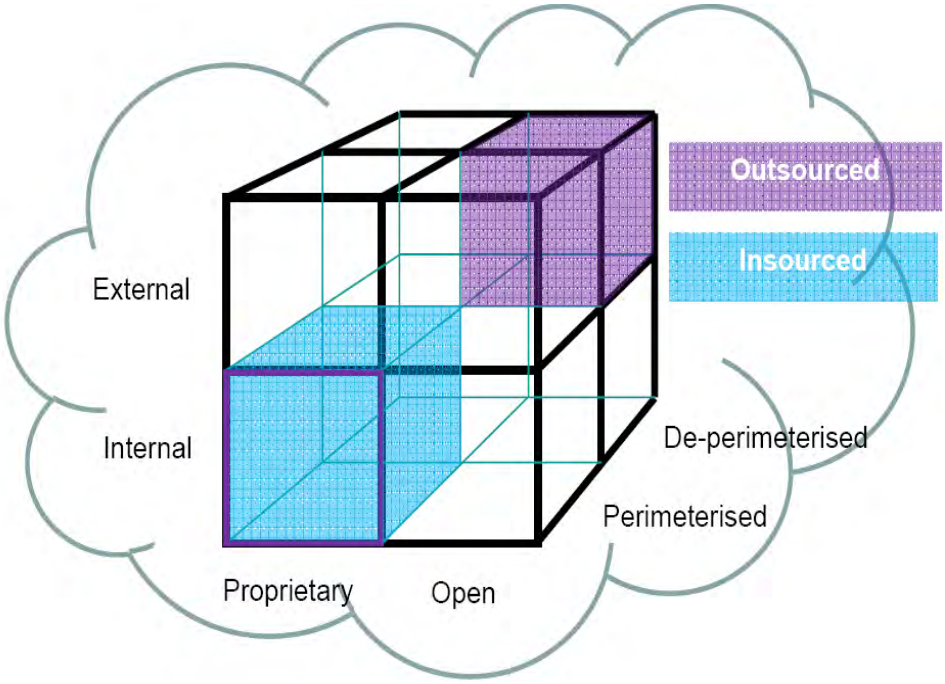

Figure 3.2: The cloud cube model (JERICHO, 2009).

However this model does not address the issues of how trust is developed between customer and service provider. It helps organisation determine which services can be outsourced to the cloud, but leaves the issues of trust to be negotiated between customer and service provider based on customers understanding of the cube model.

A review of these models shows that there is need for a more comprehensive model that will capture the different facets of trust and provide metrics that will help customers determine the level of trust that is to be placed on any particular provider. Also the model should be able to help the service providers measure their service and predict how trustworthy their services are or can be perceived by customers.

3.5 Conclusion

The chapter reviewed, trust in computer science its definitions and models and shown how these models come short in ensuring trust in adoption of cloud computing. We have also suggested what should be done in ensuring that cloud computing trust can be built and nurtured in cloud computing environment. Chapter 4 discusses challenges facing cloud computing adoption related the security, legal and compliances.

4. SECURITY, LEGAL AND COMPLIANCE ISSUES

4.1 Introduction

As section 1.2 and 2.1 have mentioned, the security, legal and compliance challenges affects the level of trust that a client or customer can vest on the vendor. This chapter explores the different security, legal and compliance issues raised by cloud computing and analyses how these issues are a barrier to cloud computing adoption and proposes ways of alleviating these barriers. Different security concerns related to threats and vulnerabilites are analysed. Legal and compliance issues related to data protection, privacy and regulations such as HIPAA, SOX among others are analysed and solutions proposed.

4.2 Security

In the psychology of security, Schneir argues that "*security is both a feeling and a reality. And they are not the same*" (Schneir, 2008). In this, Schneir means that, the reality of security is based on the probability of different risks and how effective the various mitigation strategies are in place in dealing with the perceived risks. Security is also a feeling based on the psychological reaction to both the risks and the countermeasures.

Therefore, this means that, cloud computing need to appeal to the feelings of the clients and address the potential security risks in a manner that clients will feel safe and secure. By addressing security is this way clients will feel safer and secure and hence trust cloud service providers. Figure 4-1 shows how security and compliance can be mapped to the cloud model as proposed by Cloud security alliance. This model helps in identifying the gaps existing between the organisations compliance model, the security control model and the cloud model. By identifying the compliance requirement and where in the security model they are required or are fulfilled the organisation can then link the appropriate security control to its appropriate cloud infrastructure.

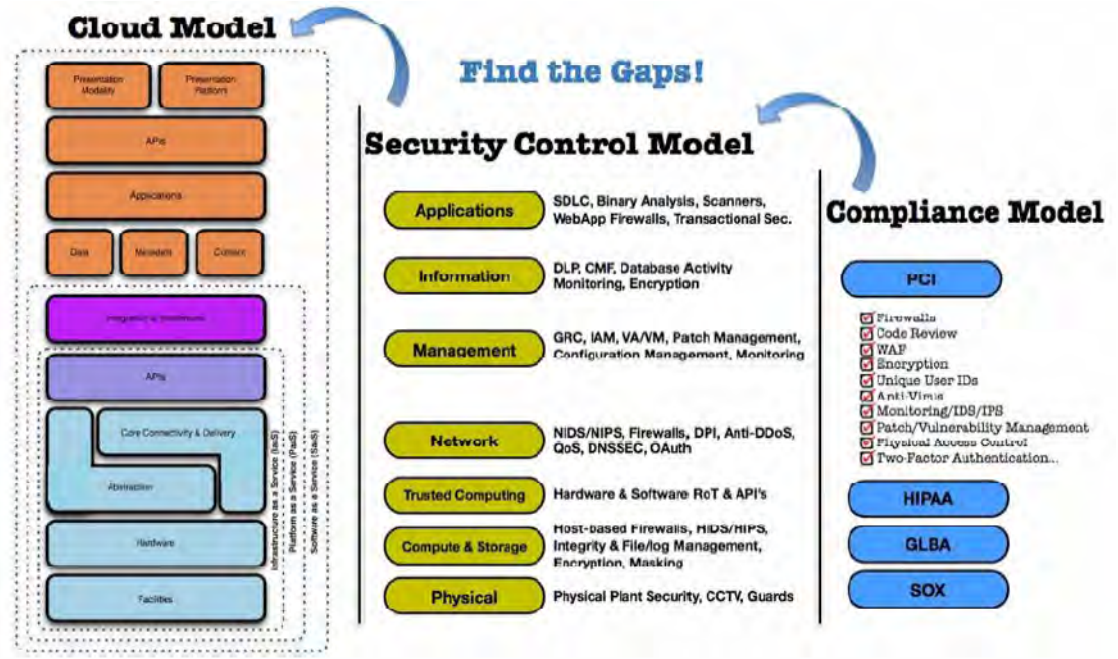

Figure 4.1: Mapping Cloud model to Security and Compliance Model (CSA, 2009)

4.2.1 Security challenges in cloud computing

Securing computer systems has not been an easy task. And for cloud computing with its multi-tenancy the challenges for security mount. Cloud computing and cloud service providers need to address a number of challenges that affects security in the cloud. How these challenges are addressed and how the mitigation plans are put in place is crucial in ensuring that clients trust cloud computing environment. The challenges that need to be addressed are as follows:

Loss of governance

By using cloud services the client passes control to the provider. This passing off, of control to the provider, results in loss of control over a number of issues which in turn may affect the security posture of the client data and applications. This is aggravated by the fact that SLAs may not tender commitment on the part of the provider, and thus widening the security cover gap. The terms of use policies also contributes as can be exemplified by Google App engine terms of use which require the user to "*agree that Google has no responsibility or liability for deletion or failure to store any Content and other communications maintained or transmitted through use of the service"(Google, 2010).*

Amazon is another example where their terms of use for their Amazon Web Services, makes it clear that they have no liability to any unauthorised access, use, corruption, deletion among other thing to the clients data or applications (Amazon, 2010). This poses challenge to customers as to how to ensure security of their data and applications which may be hosted in the cloud by a third party.

Lock-in

Lack of tools, procedures and standards for data format or service interfaces that could guarantee portability and interoperability between applications and services and between vendors is another hurdle. This will result in forcing the client to be fully dependent on the service provider.

Isolation failure

One of the characteristics of cloud computing is multi-tenancy and sharing of resources. Issue such as, failure for separate storage mechanisms and reputation between diverse tenants. It also raises question on attacks such as guest hopping attacks and how they can be dealt with.

Malicious insider

This may be the most difficult challenge to deal with in cloud computing. Although less likely to occur, damage that may accrue from it is great. This is because the architecture of cloud computing environment creates certain roles which aggravate the risk of insider attack. Examples of these roles are: the cloud service provider system administrator and managed security service providers.

Insecure or incomplete data deletion

What happens when a client requests to delete a cloud resource? Is there possibility of partial deletion? How timely is the deletion made? Given the nature of cloud computing these questions have no straight answers and in case of hardware re-use the risks are very high to clients.

Data interception

Given the distributed nature if cloud computing architecture, the amount of data in transit is increased greatly as opposed to conventional computing environment. This makes cloud

computing more susceptible to attacks such as: replay attacks, man-in-the-middle attacks, sniffing and spoofing.

Management interface compromise

With the interface to cloud services is Internet based, and allows for remote access to resources by the use of web browser, this increases the risks of malicious activity (Jensen and Schwenk, 2009). Given the vulnerabilities of web browsers, the possibility of service manipulation is great. For example, the provider may control all the operations or the customer may take control of a number of virtual machines in the cloud.

There are other possible security challenges such as: data leakage during upload or intra-cloud transfer, distributed denial of service attacks, economic denial of service attack, loss of encryption keys, undertaking of malicious probes or scans, service engine compromise, conflicts between client hardening procedures and provider procedures (Jensen and Schwenk, 2009, Hogben and Catteddu, 2009, Catteddu and Hogben, 2009, CSA, 2009, CSA, 2010, Ristenpart et al., 2009).

However there are other challenges that may impact cloud computing security though they may not be directly related to it. These challenges are such as: network breaks, modification of network traffic, management issues of cloud resources such as congestion, mis-connection, and non-optimal use of resources. Also risks such as social engineering attacks, theft of equipments and natural disasters (Catteddu and Hogben, 2009).

4.2.2 Vulnerabilities and Threats in cloud computing

Cloud computing environment apart from creating challenges to security, it also increases the vulnerability and attack surface. The vulnerabilities and threats that cloud computing need to address among others are as follows (Catteddu and Hogben, 2009):

- Poor authentication, authorization and accounting system.
- User provisioning and de-provisioning; the ability of customer to control the process.
- Remote access to management interface.
- Hypervisor vulnerabilities such as virtual machine based rootkit.
- Lack or weak key encryption.
- Lack of standard technologies and solutions.

- Poor key management procedures.
- Inaccurate modelling of resource allocation.
- Mis-configuration.
- Lack of control in vulnerability assessment process.
- Possibility of internal network probing in the cloud.
- Service level agreements with excessive business risks, conflicting promises to stakeholders.
- Possibility of co-residency checks occurring.
- Lack of audit or certification on part of cloud service provider.
- Lack of forensic readiness, sanitisation of sensitive data.

This list is not intended to be exhaustive but it shows the importance of addressing security issues for trust to be built for cloud computing customers. As for the threats, the Cloud Security Alliance (CSA, 2010) has identified what it calls the top threats to cloud as follows:

- Abuse and nefarious use of cloud computing.
- Insecure interfaces and application programming interfaces (API).
- Malicious insider.
- Shared technology issues.
- Data loss or leakage
- Account or service hijacking.
- Unknown risk profile.
-

Though the threats identified are representative of all the possible threats that can occur in the cloud, nevertheless they portray the necessity of security to appeal to the feelings of the clients. This is because without security addressing the reality of these risks and providing for mitigation plans, clients trust for cloud services will be hard to build.

4.2.3 Cloud computing: source of perceived security threats

With the different security challenges, vulnerabilities and threats facing cloud computing, fear raises in the potential clients of cloud computing. This creates distrust as to cloud computing from clients and hinders/slows down adoption of cloud computing. In this section a brief dissection of some of the sources of the perceived threats resulting into trepidation is done. The most common threats (Andert et al., 2002, Armbrust et al., 2009, Catteddu and Hogben, 2009, Chow et al., 2009, CSA, 2009) are described below:

Confidentiality: This raises questions such as how will sensitive data stored in the cloud be? Will the cloud not leak or compromise confidentiality of clients' confidential data? These questions and other of similar nature are linked to the fear of loss of control over data

stored in the cloud. Thus, this calls for security mechanisms in the cloud environment which will appeal to clients feelings related to confidentiality.

Integrity: This related to the clients need to be sure that, the provider is performing the right kind of operation on data. It also relates to the need for assurance that data stored or processed in the cloud has not been tampered. This calls for the need of integrity mechanisms which are transparent without compromising security.

Availability: What happens if cloud service provider is attacked? Will the customer loose business? What happens if the provider files for bankruptcy? Or is acquired by a new management? These questions relate to the issues of disaster recovery and business continuity. This calls for cloud computing service providers to have a mechanism which assures clients of business continuity.

Privacy: What happens when provider performs data mining on clients' data? An example being Google mail (Gmail). Will the results of the data mining on the clients' data not be revealed to a third party?

Increased attack surface: How does cloud respond to phishing attacks? As communication is via the Internet, will the attacks now be targeting the communication link?

Auditability and forensics: how will data be audited? Who will perform the audit? With data in the cloud, how can forensic and e-discovery be performed? Who will be responsible for forensic and e-discovery? The client or the provider?

Legal quagmire and transitive trust: is the customer or the service provider responsible for compliance? What happens if the service provider subcontracts? Should the customer trust the subcontractor?

Even though the fears are based on the conventional computing environment, in order to be able to build clients' trust, these fears highlight the need for service providers to adapt well known security mechanisms or techniques. They also call for research and innovation in security techniques and technologies in order to ensure that cloud computing is secure and hence trustworthy.

4.2.4 Security and cloud computing (Standards and Best Practices)

With all the fears surrounding information security and cloud computing in particular, in this sub-section a review of a number of security standards and best practices that have been developed and used in conventional computing is done. The review aims to identify and see how these standards and best practices can be used in ensuring cloud computing security and build trust.

ISO 27001 (BS ISO/IEC 27001:2005, BS 7799-2:2005)

This standard which was formerly was known as BS 7799-2, is intended to "*provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system (ISMS)" (BSI, 2005 a).* The standard defines how a business or an organisation can organise it information security, based on it needs, objectives and security requirements. The standard also can be used by both internal and external parties in assessing the security posture of an organisation; this has led to certifications showing that an organisation meets the standards requirement for information security. The certification is an indication that the organisation has implemented information security in the best possible way. However, certification for cloud computing may not very useful. This is because the client and vendor security requirements and practices may differ which will still require vendor to adjust their practices to meet clients' needs. Nevertheless, vendor certification is still important as an indication that they are committed to ensuring security and use of security best practices.

The standard prescribes how information security can be managed through ISMS. The management system has four phases which are: the Plan phase which is dealing with the planning of organisations' information security; sets objectives for information security and selects the appropriate security controls. The standard contains one hundred and thirty three (133) possible controls. The second phase is the DO phase which executes all that which was planned in the planning phase. The third phase is the check phase. This phase supervises how the ISMS functions and monitors to see if the results meets the set objectives. The fourth phase is the Act phase, which is concerned with taking of corrective measure for anything that was identified in the previous phase as not meeting the objectives. Figure 4-2 shows how these phases are related.

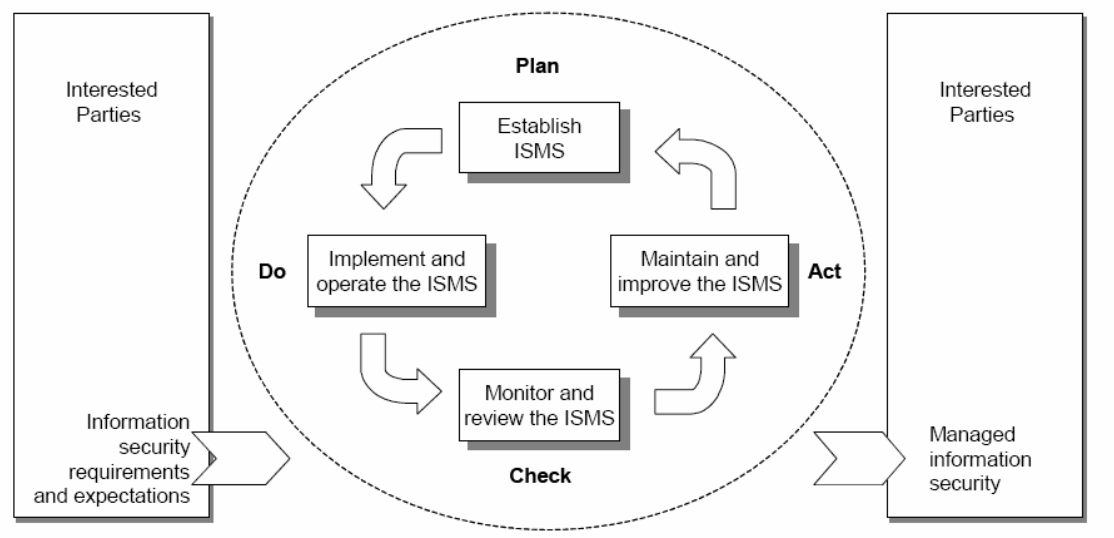

Figure 4.2: The four phases of ISO 27001 (BSI, 2005 a)

The standard also requires a set of documentations to be produced as a result of complying with the standard. These documents are: the scope of the ISMS, the ISMS policy, procedures for document controls, internal audit, and procedures for corrective and preventive measures, documents relating to the selected security controls, risk assessment methodology, risk assessment report, risk mitigation plan and records. However, the amount and complexity of the document will depend on the size of the organisation and the complexity of the ISMS.

In order to address security and trust issues in cloud computing adoption, we propose that, vendors and clients should work together in the whole process of developing and implementing ISMS. This will enable both parties to understand the security requirements and capabilities of the vendor in providing the required security and hence will facilitate and foster trust.

ISO 27002 (BS ISO/IEC 27002:2005, BS 7799-1:2005, BS ISO/IEC 17799:2005)

This standard is an auxiliary standard to ISO 27001. It establishes the "*guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation*"(BSI, 2005 b). It purpose is stated as "*provide general guidance on the commonly*

accepted goals of information security management" (BSI, 2005 b). The objectives and controls in this standard are expected to meet the requirements identified during risk assessment when implemented. The standard can be used by an organisation as a basis for developing organisational security practice guidelines and security standards that will be vital in fostering inter organisational trust. The standard covers areas such as data security, data processing, data transmission, computers, information exchanged, risk management, access control, information system acquisition, incident response and business continuity.

By using the guidelines outlined in this standard, the cloud vendor and client need to work together to identify how the different ISMS requirements can be implemented in adopting cloud computing services, and how issues related to access control, incident response and business continuity will be tackled. This collaboration between service providers and clients in the process of developing and acceptable security posture is important in facilitating trust and adoption of cloud computing. Therefore, by leveraging the ISO 27001 and ISO 27002 information security standards and by working in collaboration with clients in developing a set of transparent security principles vendors can build customer trust and thus enhance the adoption rate of cloud services.

Nevertheless, these are not the only standards. There are other standards such as the ISO 27005 (BSI, 2008) which helps in conducting security risk management in support of the requirement for ISO 27001. Another standard is the BS 25999-2:2007 (BSI, 2007), that deals with specifications for business continuity management. Other standards include the NIST SP800-50, PCI DSS.

Therefore, through collaboration and the use of these different security standards, clients and vendors can manage to establish security policies and best practices to govern their relationship. It is through collaboration a structured security and trust framework can be developed that can be useful in assessing the security requirements of the user and the ability of the

vendor to meet those requirements. In this dissertation a proposed trust framework for cloud computing based on the different standards discussed in this section is given in table 4-1.

Security and trust Framework for Cloud computing Adoption

Security Objective	Description	Trust Objective	Outcome
Security Policies	Outlines the organisation guidelines and mandates for information security	Sharing on security requirements, policy, standards, rights and responsibilities	Agreed upon security policy, standards and practices
Organising Information security	Governance structure for both internal and vendor or third party service provider	Agreements on how information security, legal and compliance issues are handled	Auditability and accountability between both parties.
Asset Management	Identification, organisation and management of IT resources	An agreed upon methods or means for both manual and automated for security, legal and compliance management	Agreed upon methods for managing the IT resources to ensure security, legal and compliance management.
Human Resource security	Managing personnel and access rights, security training and awareness	Develop HR management policies, standards and operating procedures	Reliable and reasonable expectations on personnel behaviour and activities
Physical and Environmental security	Physical protection of IT resources	Share on physical control measures for IT infrastructure protection	Assures that the infrastructure is properly protected
Communication and Operations Management	Guidelines on how security is managed and incidents communicated, standard operating procedures	Develop capabilities, operating procedures for security and data management. Develop/share on techniques used in security management and system monitoring	Reliable/trusted cloud infrastructure facilities, meets specific customer requirements, an understanding for the need for complementing security controls.
Access Control	Authorisation and authentication procedures to IT resources and data	Develop/agree on authorisation and authentication mechanisms, the technology used and standards	Meeting customer requirements for access control.
Information System Acquisition, Development and Maintenance	Acquiring of information for system/application development and maintenance	Share/develop standard, procedures to ensure secure acquisition or development of systems or applications	Assures of the effort put in the process of development of systems, and how reliable the security measure or control used are.
Incident Management	Procedures for managing and reporting security events and problems	Decide on policies, procedures and standards for managing incidents, how vendor/customer is notified and/or the general public or authorities	Customer involvement in incident management and disclosure, resolution and an understanding of the providers ability for incident response management and report
Business Continuity	How IT disaster recovery planning and business continuity are related with	Agree on/ develop standards, procedures for disaster recovery, business continuity.	Determines if the vendors existing standards and procedures are

	contingency planning.	Agreement on SLAs for down-time and data processing priorities.	sufficient for the customers' needs and SLA requirements
Compliance	For both legal and security standards, policies and best practices	Vendor/customer share/work on applicable certifications, auditing, assessment to ensure the required level of compliance is met	Determines the responsibility and level of accountability between vendor and customer for the required compliance levels.

Table 4.1: Security and Trust Framework for Cloud Computing Adoption based on ISO 27001 and ISO 27002 (Author)

The use of this framework in cloud computing will enable clients and vendors to manage security risks, decide on how risks are mitigated and controlled, and address compliance and regulatory requirements effectively. The framework also serves as a means for measuring the level of trust that have been achieved between the client and the vendor, as it shows which information or data can be shared and the responsibilities for each party in the relationship. The expected benefits of using this framework are such as: increased trust between service provider and client; allows for comprehensive set of security best practices to be used in ensuring information security; fosters customer trust when used by vendor as it can be independently verified or certified and audited by a third party; it simplifies compliance as it is founded on standards that are designed to be used on most IT environments; assures the client of acceptable levels of confidentiality, integrity and accountability; enables the vendor to manage properly clients security expectations and requirements; and it reduces the management overhead and costs related to compliance assurance and risk management for both parties

Control Framework for Information and related Technology (COBIT)

This is a "*framework for IT governance and control, it supports toolset that allows managers to bridge the gap between control requirements, technical issues and business risks*" (ISACA, 2010). As a governance and control framework COBIT provides two procedures one for defining an IT strategy and the second for managing third party services. It also provides a maturity model that can be used to assess the maturity of the IT governance processes in an organisation.

For cloud computing clients, by using the COBIT procedure the client will be able to determine what should be done before and after selecting a cloud

vendor or solution. COBIT will also help, in monitoring the value that is to be gained by adopting cloud computing, the level of risk exposure and in deciding who will be responsible, accountable, consulted and informed during the cloud adoption project.

The maturity model will help an organisation in determining the level of maturity of its IT governance, and whether the maturity level is acceptable for the move to cloud computing. Therefore, by using COBIT organisation can institutionalise good practices which will ensure that IT investments produce business value (ITGI, 2007). And in this case it will help in ensuring that the move to cloud solutions will result in better business value without compromise. Figure 4-3 shows the overall COBIT 4.1 framework

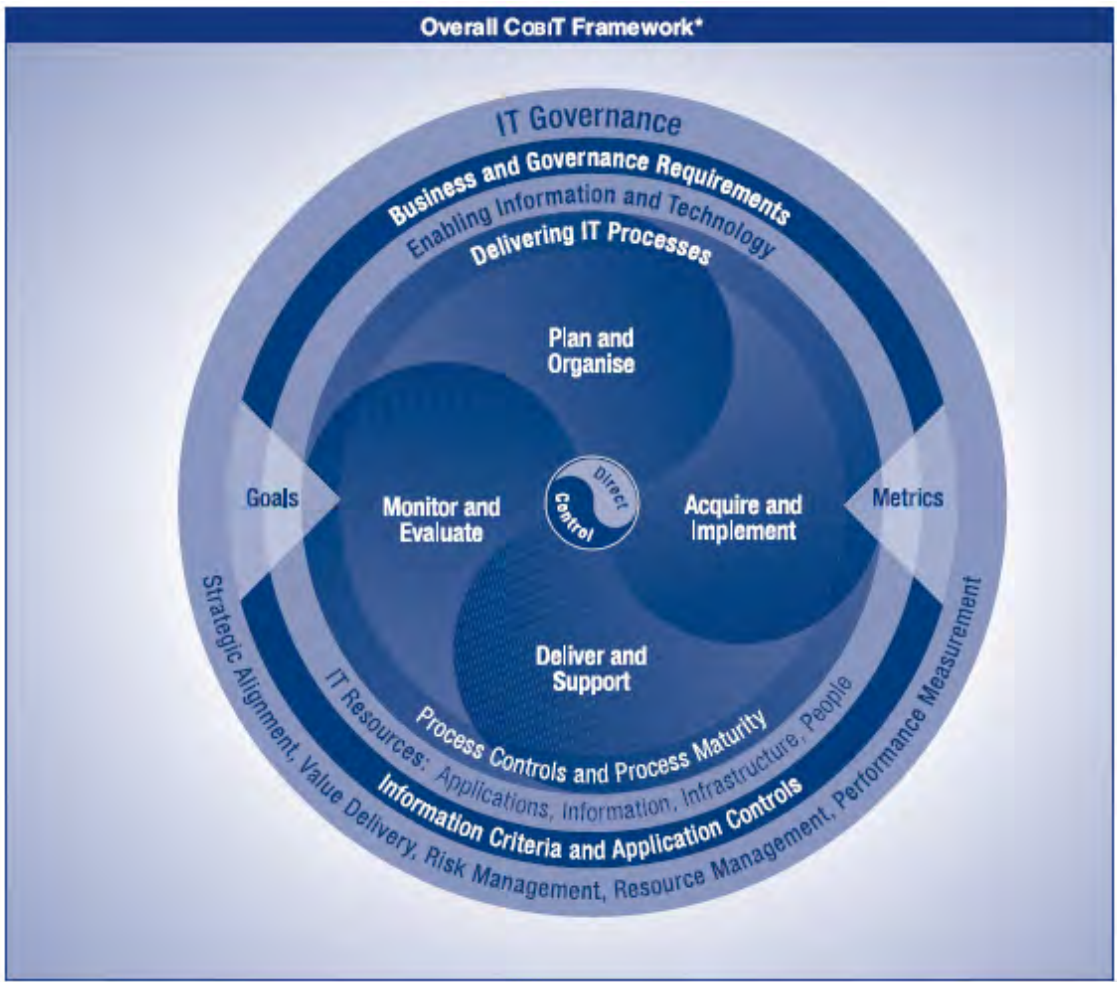

Figure 4.3: Overall COBIT 4.1 Framework (ITGI, 2007)

By using this framework an organisation can try to answer questions related to governance and best practices and determine whether the organisation is capable of IT governance in the cloud.

The Information Technology Infrastructure Library (ITIL)

Is a set of best practices that are documented for the purpose of supporting IT services management. The practices have been codified into books covering different aspects of IT management. The topics covered in ITIL include service support, service delivery, Information and Communication Technology (ICT) infrastructure management, Security management, Business alignment, application management and ICT asset management (OGC, 2010).

Open Security Architecture

The standards and best practises discussed so far pre-dates' the cloud computing error. The cloud computing pattern developed by the open architecture is an attempt at addressing the different security and migration challenges facing cloud adoption. As figure 4-4 shows, the pattern have combined different possible aspects of cloud use and how these can be managed and monitored. The pattern also provides mapping of the different aspects of security and management to ISO standards and COBIT best practices for IT governance. The pattern also identifies different stakeholders and their respective responsibilities.

Standardised security framework for cloud computing

As it have been shown, the biggest problem with cloud computing security is lack of transparency of cloud vendors about their security capabilities, and lack of standard or framework for security. As a result of this different organisations are currently working in developing different security frameworks for cloud security . Frameworks in development (Mather, 2010) include: A6, Trusted cloud initiative, Common Assurance Maturity Model (CAMM) and Federal Risk and Authorisation Management Program (FedRAMP).

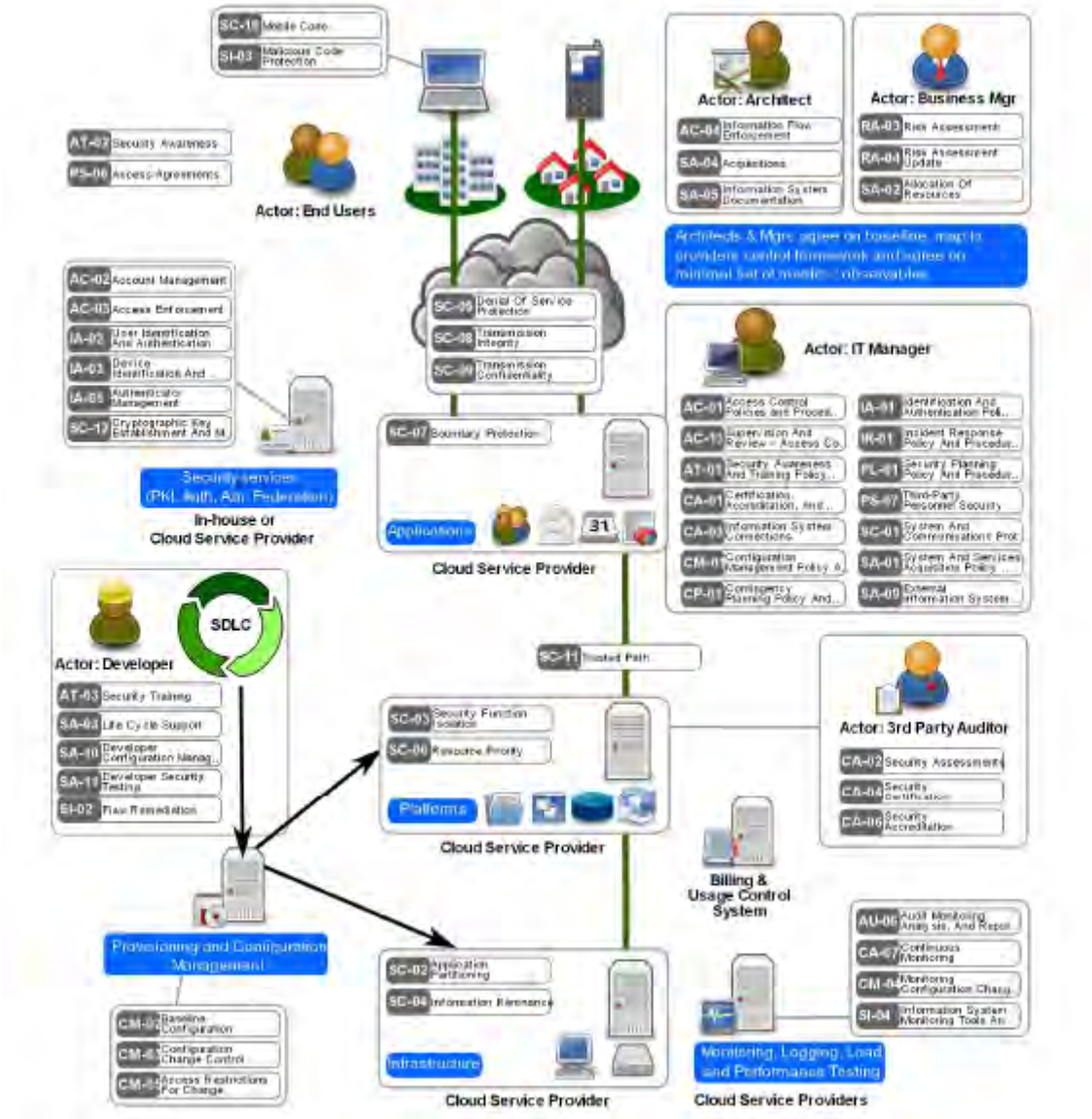

Figure 4.4: Open Security Architecture-cloud computing patterns (OSA, 2010)

A6 (Automated Audit, Assertion, Assessment, and Assurance API) working group

The effort is known also as Cloud Audit, and is under the leadership of Chris Hoff of Cisco Systems.

Trusted Cloud Initiative

This initiative is under the Cloud Security Alliance; it is chaired by Liam Lynch eBay security strategist. The objectives of the initiative are to provide a reference framework for implementation and enable end-to-end security platform.

Common Assurance Maturity Model (CAMM)

This is a consortium of made up of 24 members. Most of the members are vendors, but it also include the European Network and Information Security Agency (ENISA). It was launched initially as an assurance framework metric. The initiative is planning a formal release in November 2010.

Federal Risk and Authorisation Management Program (FedRAMP)

This is an initiative by the US government for continuous authorisation and security monitoring of shared IT resources or services of the federal government departments and agencies when they contract or outsource their IT services including outsourcing to cloud computing.

4.3 Legal and compliance issues

With data and application hosted by a third party, the cloud service provider; issues of ascertaining the legal and compliance impact to participating parts is difficult. Issues related to data protection, privacy, jurisdiction of storage and processing and e-discovery raise. It also raises the issue related to the responsibility of the aforementioned issues. Figure 3-5 is a map showing the differences in regulations around the world relating to data protection legislation.

The map shows, the differences in country specifics in data protection and privacy. this is shown by the level of restriction or lack thereof, it also shows where there are no legislation or where legislation is pending. The map shows also countries where the government can interfere with data protection and privacy due to surveillance. These differences in regulations and government interferences poses challenges to businesses as they seek to adopt cloud computing. For example a business located in Europe may be jeopardised by using cloud services which hosts its data in a country where there is no data protection laws or where there is legislation but it does not meet the European Union (EU) data protection requirements.

Therefore, these differences calls for business managers and chief information officers to understand how local data protection requirements of different countries may impact their business in terms of complying to their privacy and data protection legislation in country of origin.

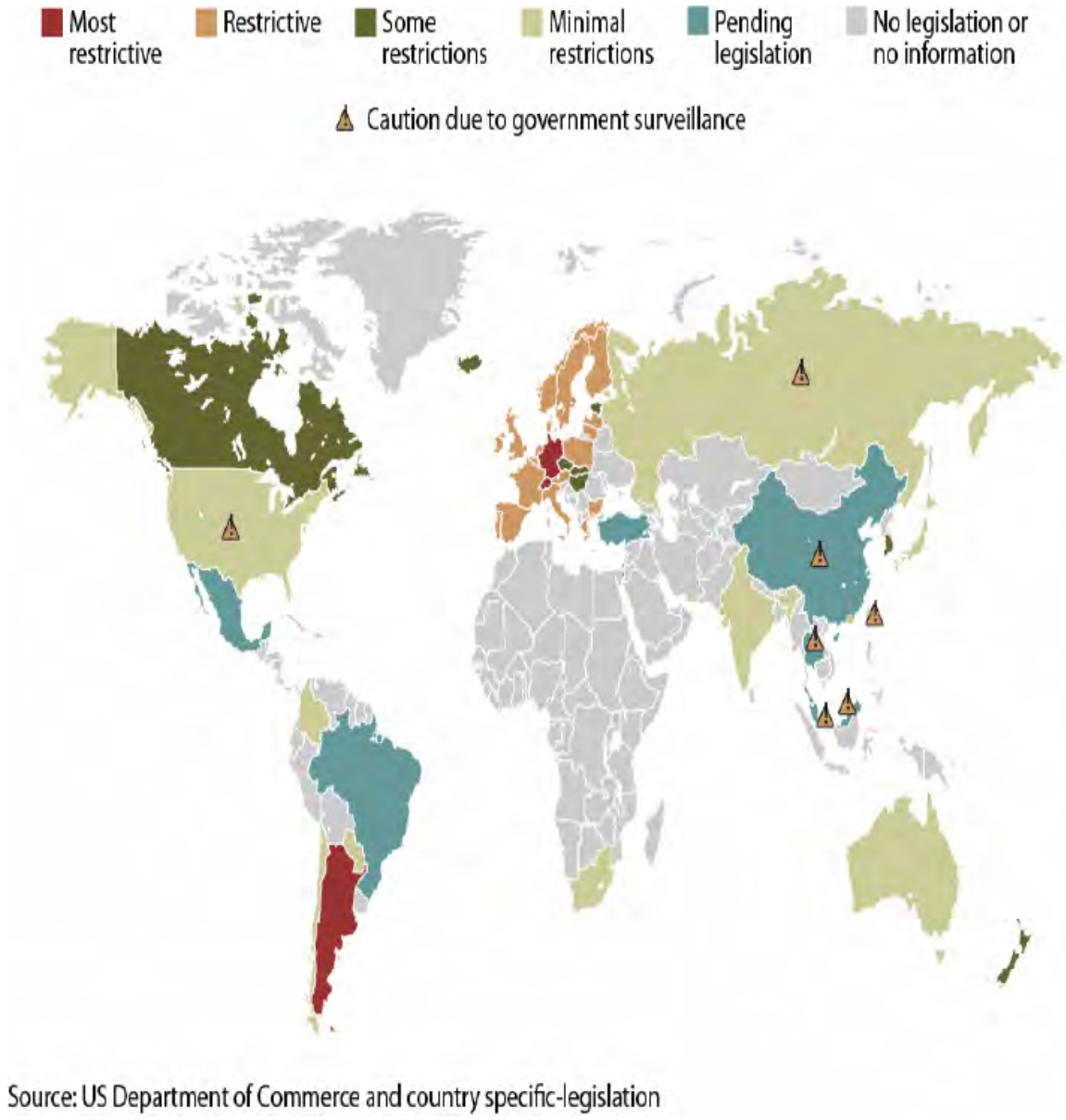

Figure 4.5: World Data Protection legislation (Forrester, 2010)

For the cloud providers, an understanding of local data protection requirements impact on their clients' data is of importance as it will help in providing their clients with accurate and sufficient information and also help in tailoring their offerings to meet their clients' requirements. How vendors respond to these legal and compliance challenges have impact on how trustworthy the vendor is/will be perceived by customers in handling legal and compliance requirement and needs of the customer.

4.3.1 The Legal framework

For cloud service customers and providers in Europe (EU), the EU Data Protection Directive 95/46 is more relevant (Mather *et al.*, 2009, Hustinx, 2010). For those in the United States of America (US) there is no specific directive or law but a number of regulations have bearing on their businesses (Mather *et al.*, 2009, Jaeger *et al.*, 2009, Sotto *et al.*, 2010). For other parts of the world as the map in figure 3-5 shows may have national regulations or no regulations at all for data protection. All these differences pose challenges for both cloud customers as well as vendors in deciding whether to use cloud services for the case of a customer and where to locate the cloud in the case of a vendor.

The EU directive clearly defines the obligations which are mandatory and binding to all who process personal data (Hustinx, 2010, EC, 2006, Robinson *et al.*, 2009, Warren and Brandeis, 1890). Therefore, the directive is applicable for cloud service whenever personal data processing is involved and falls within the EU jurisdiction (EC, 2006, Hustinx, 2010, Widmer, 2009, EU, 2006), the case is not much different in the US only that the vendor or customer may have to comply to different laws and regulations (Sotto *et al.*, 2010). The EU directive articles 6 and 17 shows that cloud computing services are not exempt from compliance to data protections laws which provide for individual privacy and personal data protection. The articles provide for the security obligations of the data controllers and data processors with the responsibility for both technical and organisational measures that ensures privacy. They also limit how personal data can be collected and processed to the purpose for which they were initially collected. These two articles apply to cloud computing in that they limit how cloud vendors or customers can collect, and process personal data (EU, 2006).

However, this is easy said than done. Although the principles derived from the EU data protection Directive are applicable, technology independent and the legal framework is viable, there remains challenges in applying these principles in cloud computing. The main reason being that the directive was made when technology was still in its early stages and could not envision cloud computing. The case is the same for the US as providers and customers need to comply with the various regulations that are applicable. For the rest of the world the case may not be that difficult but problems arise when there is the issues of data

transfer, especially when it involves the EU. Section 4.3.2 addresses some of the main challenges in the legal arena of cloud computing.

4.3.2 Legal challenges

From the legal framework of section 3.3.1, a number of challenges emerge relating to cloud computing. These challenges may be categorised under various names and titles. For example Sotto, et al (2010) identifies some of the challenges as Privacy and security laws issues, service provider restrictions, state Information security laws, EU regulatory issues, International data transfers and legal base for processing data in the cloud. Dr. Widmer (2009) identifies the challenges as commercial, open issues on data protection, and contractual issues. In this section the challenges are identified as; the role of the cloud service customer/provider, the applicability of EU laws, trans-border data transfers, ensuring data protection. We see these challenges covering most of the legal aspects of using cloud services.

The first challenge: the cloud service customer/provider role; the EU directive puts on the shoulders of data controllers most of the obligations for ensuring privacy and data protection of the individual, with few on the data processors (EU, 2006, Hustinx, 2010). In the case of cloud computing it is hard to pin cloud providers as data controllers though they process data entrusted to them by the data controller according to the directive. Therefore it is imperative that the role played by cloud vendors and customer be clearly defined to ensure compliance to the directive.

The second challenge: the applicability of EU laws; this relates to how cloud vendors will be made to comply with EU laws. Will they need to have their cloud in the EU? Is it mandatory the cloud be located in EU or a country that is compliant? How is this going to be verified?

The third challenge relates to trans-border data flow. The directive demands that data not be transferred outside the EU. Transfer can only take place to countries with adequacy level of protection. It also demands for contracts and notifications in case of transfers taking place. The problem in this case lies in the directive definition of data transfer. The definition is based on a point to point concept of data transfer. With this concept it is difficult in cloud

environment to constantly notify and sign contracts as data tend to be constantly moving and changing jurisdictions.

The fourth challenge is that of ensuring the protection of data. The challenge here is to ensure that both data controller and data processor have effective means of protection for data.

4.3.3 Compliance issues

Nature of cloud computing environment puts at risks industry and/or regulatory requirements. This is because of the difficult to force providers to comply with these regulations or industry standards. For example in using public clouds infrastructure it entails failure to comply with certain requirements such as PCI DSS, Federal Information Security Management Act (FISMA) of 2003, Gram-Leach_Billey Financial Services Modernisation Act of 1990 and the European Data Protection Act of 1990 among others. Figure 4-6 shows the main players in ensuring compliance and how they are related.

This is made difficult because these acts and regulations were not prepared with cloud computing in mind. They focused of physical asset protection (Hamilton). Compliance is also made difficult as vendors are not necessarily industry specific. This means that vendors may not be required to comply with any industry specific legislation or standard. Another aspect is that vendors may be offering their services to customers from different industry with different compliance requirements.

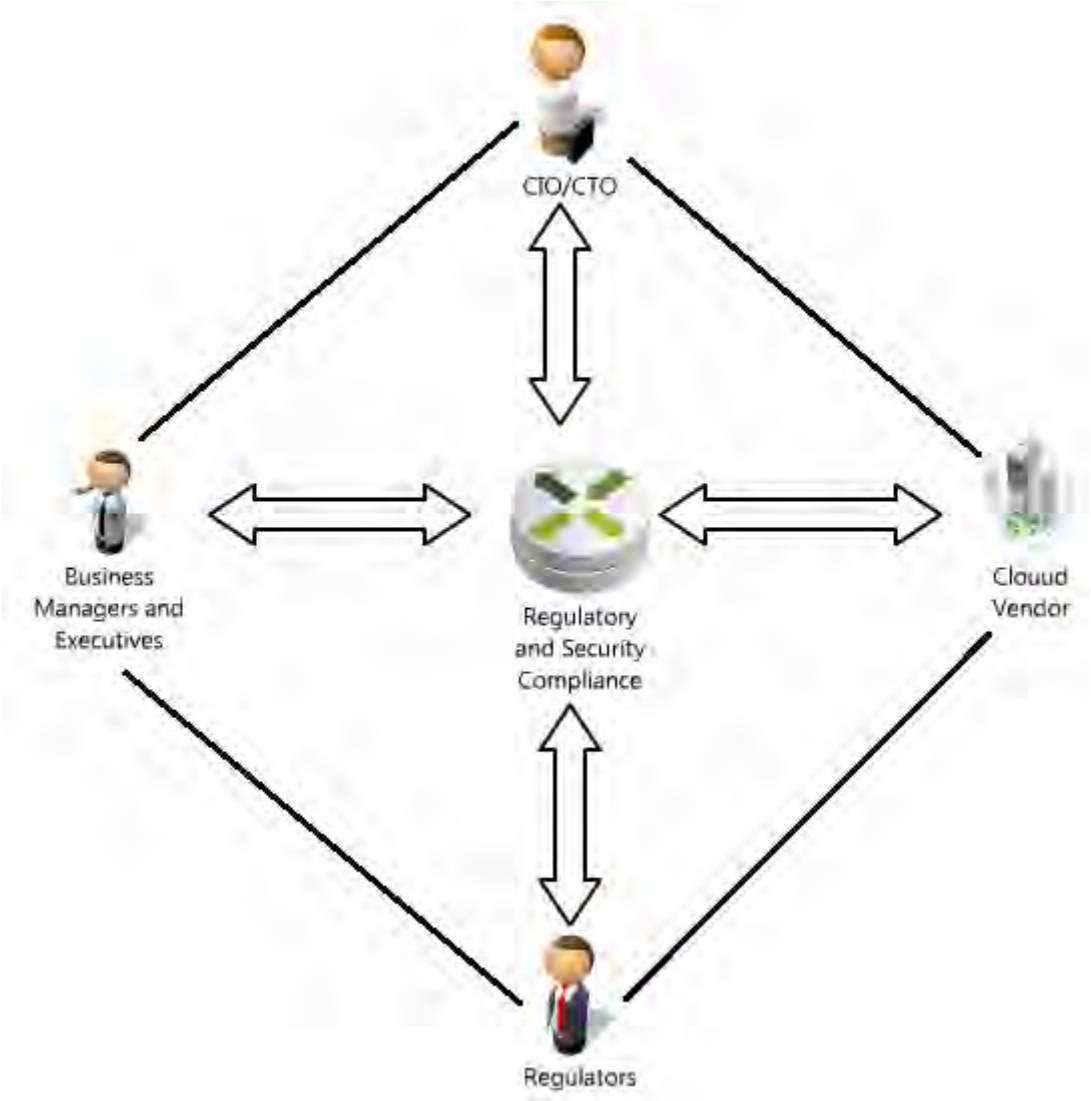

Figure 4.6: Cloud computing compliance main Stakeholders relationship (Author)

4.4 Conclusion

This chapter have identified different security, legal and compliance issues in cloud computing adoption. An analysis of security challenges, the fear that results from these challenges , the legal issues related to data protection, trans-border data flow and compliance to different legislations and industry standards that pose challenges to adopting cloud computing. Also proposed a security and governance framework for cloud computing based on security standards and the COBIT best practices. Chapter 5 will discuss different organisational challenges in adopting cloud computing.

5. ORGANISATIONAL FACTORS IN CLOUD COMPUTING

5.1 Introduction

This chapter discusses the organisational factors that are important in cloud computing adoption. Large organisations are more concerned with the value that cloud computing may offer to them rather than just the migration of applications or using cloud computing just as a platform for service delivery. This section will identify and discuss issues surrounding organisation adoption and migration of applications/systems to the cloud in order to satisfy and meet organisations requirements. Chapters 3 and 4 have identified the trust, security, legal and compliance issues that organisations faces in making a decisions towards cloud computing, this chapter will address the organisational changes that may be a result of moving to the cloud. It will also address issues related to IT governance in the cloud, risk management, migration challenges, SLAs and costs implications of cloud to the organisation.

5.2 Organisational change

The IT department in organisations are the ones that are going to be greatly affected by the adoption of cloud computing (Mather *et al.*, 2009). These departments are used to having control over different aspects of organisation IT infrastructure operations and management. These departments controlled such things as IT procurement, IT asset management, security control and billing (Khajeh-Hosseini *et al.*, 2010a). With cloud computing this is about to change. In 2008 Nicholas carr argued that the mode of IT service delivery resembles in some aspect that of electricity delivery in the early days of electric invention (Carr, 2008). During that time every manufacturer had to generate their own electricity regardless of the type or nature of their business. In the same respect today's business organisations build their own IT infrastructure regardless of their business (Carr, 2008, Khajeh-Hosseini *et al.*, 2010b, Khajeh-Hosseini *et al.*, 2010a). This trend results in inefficient IT infrastructures (Economist, 2008). Cloud computing is about to change that. This will be possible through cloud computing provision of facilities such as computational power, storage capacities and offer these as utility services.

However, the IT department of most organisations are not used to utility model of service sharing. This type of utility billing for shared resources in an organisation calls for changes in organisation culture and organisation process maturity (Khajeh-Hosseini *et al.*, 2010b, Fellows, 2008). (Elson and Howell, 2009) provide example of how cloud could affect the IT department. In their example they describe how cloud could help in conflict resolution in system development roles. The effect of cloud computing to the Authority of the IT department is discussed in *from users to choosers: The cloud and the Changing Shape of Enterprise Authority* (Yanosky, 2008). Knode, R reports a case illustrating authority of the IT department being by-passed (Knode, 2009).

Therefore, an organisation planning for cloud computing adoption should make effort to access and analyse all the possible organisational impact to culture, processes, work relationships and internal politics that cloud computing may bring.

5.3 Governance and risk management

With the organisational changes that are imminent from adoption of cloud computing as discussed in the previous section, governance and risk management of It resources in the cloud environment is another challenge facing organisations. Effective management of IT resources in cloud environment and risk management should be a result of an organisation having a well developed IT resources and information security governance processes, as part of the organisations' corporate governance obligations (CSA, 2009). The results of a well developed governance processes are information security management processes that are flexible, repeatable, measurable, sustainable, defensible, cost-effective on an ongoing basis (CSA, 2009). For cloud computing the main concerns to organisations in relation to governance and enterprise risk management is how the organisation can identify and implement appropriate organisational structures, processes and controls to ensure that there is effective information security governance, risk management and compliance (CSA, 2009, Buyya *et al.*, 2009, Armbrust *et al.*, 2009, Golden, 2009). The governance and risk management requires organisations to ensure that there are proper mechanisms and processes across the information supply chain that covers cloud providers, customers and other stakeholders, and supporting third parties to vendors (Golden, 2009, CSA, 2009).

In order for organisations to ensure effective governance and risk management, there is a need for both vendors and customer to collaborate in developing appropriate organisational

structures, processes which will ensure good governance and risk management. But this is not an effortless endeavour as it is not likely for vendors to be able to develop these processes with every customer without jeopardising their ability to offer their services. The Cloud Security Alliance (CSA, 2009) offers a number of recommendations.

5.4 Systems and application migration

For start-ups migration of applications is not a challenge as the organisation starts by using cloud computing from the start. On the other hand, business which are already established, have a large number of systems and applications that are a result of a long period of time in business. In most cases these systems have been developed and depend on a number of different technologies, are owned by different departments or sections of the organisation, and have complex dependencies between the systems and the data they use. The business processes of the organisation also evolve to make use of the systems and are dependent on the systems. This results in a situation whereby no department or section of the organisation that has full knowledge of all the systems working in the organisation and the dependencies within them (Khajeh-Hosseini *et al.*, 2010a, Cloudcomputing, 2010).

Moreover, the development and deployment and use of IT Systems and resources is affected by organisations politics. For example, the organisation top management may set IT policies but the implementations of these policies are left to individual departments. As a result of the freedom on deciding how to implement policies, departmental managers tend to decide and adopt strategies that best suits their departments (Forbes, 2010, Khajeh-Hosseini *et al.*, 2010a, Cloudcomputing, 2010). For cloud computing, migrating systems and applications poses a challenge to organisations. The challenges include IT policy formulation, organisational politics and culture. It also includes identifying the system dependencies and how the migration to cloud will affect these dependencies and the work processes in place. Other challenges involved with migrating systems and applications to the cloud are security, compliance, and SLAs management.

5.5 Service level Agreements (SLA) management

The need for specific SLAs is another challenge. This is a challenge due to the fact that vendors may not always meet the requirements for SLA of an organisation. The potential for

down-time and lack or inadequate SLA agreement from some cloud vendors pose ac great challenge (Google, 2010, Golden, 2009, Amazon, 2010).

5.6 The Economics of Cloud computing

One of the appealing benefits of cloud computing is its payment model where the customer pays for what they use. Another closely related characteristic is the removal of investment costs for using cloud services whereby the customer is not required to invest in purchasing the IT infrastructure. However, how organisations can benefit from this utility model is not very clear. The challenges being the management of costs and the calculation return on investment (ROI) (Golden, 2009). Another challenge is that of comparing capital expenditure (CapEx) against operational expenditure (OpEx) (Buyya *et al.*, 2009, Armbrust *et al.*, 2009, Khajeh-Hosseini *et al.*, 2010a, COMSCI, 2010).

How organisations are going to benefit from the economies of scale promised by cloud computing is among the research challenges. Different researches have been carried out that have addressed the issues related to costs of using cloud computing from both the customer and vendor perspectives (Khajeh-Hosseini *et al.*, 2010a, Buyya *et al.*, 2009, Armbrust *et al.*, 2009, Klems *et al.*, 2009, Greenberg *et al.*, 2008, Barroso and Hölzle, 2009, Kondo *et al.*, 2009, De Assunção *et al.*, 2009, Raghavan *et al.*, 2007, Weinhardt *et al.*, 2009).

However, as Khajeh-Hosseini *et al, (2009)* has pointed out, the challenge facing organisations is a result of their current systems which are based "*on scaling up demands to more powerful servers rather than scaling out to large number of servers"*. Hence changing of these architectures to support the new cloud computing architecture for scaling of resources will inevitable be more expensive. With scaling out is the issue of licensing (Khajeh-Hosseini *et al.*, 2010a, Dalheimer and Pfreundt, 2009), faces the organisations as most of the software and applications used are licensed for a specific number of instances. For example, Application X may be licensed for a specific number of users and hence the organisation will have negotiated or purchased licenses for that specific number of users. Therefore, if X is to be run in a cloud platform there is need for dynamic licensing for X, and the practical implementation for this is still questionable.

Other challenges include the capital and operation costs ownership within an organisation. This is because in most organisations the costs related to capital and operations of IT

infrastructure are de-centralised and thus are owned by different departments. Another challenge related to the procurement as the current practice is for the procurement costs to be known or determined in advance for approval of purchases, with cloud computing this practice is not feasible as the model for procurement is dynamic based on demand. Furthermore, in traditional IT environment purchases are done after approval by signatories, this call for dynamic approval which is not feasible. The utility model of cloud computing, introduces a factor that is not found in the traditional computing IT as it relates to usage and billing. This factor is the uncertainty relating to the usage pattern which makes hard for current procurement practices to account for. As it has been argued in section 4.2 above, cost management calls for organisational changes in the budgeting, procurement and cost ownership procedures and process. Khaje-Hossein *et al* (2010), provides an illustrative example where the current procurement practices may fail when a critical business application reaches its cost limit and stops working.

Currently, providers do not have features that support the way costs and usage is billed within organisations and this poses a challenge for organisations. The providers charge the organisations for its usage but are not able to charge different departments of the organisation based on their usage.

5.7 Conclusion

This chapter discussed the different challenges facing organisations when planning for cloud computing adoption. The challenges discussed are: the impact of cloud computing to the organisation. These include the changes to the organisation culture, politics and organisation structure. Other organisation impact includes organisation work procedures and process that have developed over time. Another organisational challenge that have been discussed is the governance and risk management in cloud computing. This includes how organisation can mitigate risks and maintain IT governance in cloud computing that will ensure compliance to both legal and security requirement. In system and application migration challenge, issues such as organisation politics and ownership, system and application dependencies which may affect how applications are to be migrated to the cloud. In service level agreement management the issue of lack of proper SLA or inadequate SLA impacts on how organisations will use cloud computing while ensuring quality service to customers and without breaching any legal and security compliance. In the economics of cloud computing

issues related to pricing and payment models, and internal management of costs are critical. The impact of outsourcing to cloud computing of IT resources procurement was also discussed. Chapter 6 discusses the survey and its results findings.

6. CLOUD COMPUTING ADOPTION ISSUES SURVEY

6.1 Introduction

Chapters 2, 3, 4 and 5 have covered much of the research problem questions through literature review; however, an understating of the problem from the practitioners point of view is invaluable. In order to achieve this, a survey was conducted with the aim of understanding the challenges facing business managers and IT managers in their endeavour of adopting cloud computing. In order to get a proper understanding two types of questionnaire survey were conducted. The first questionnaire survey focused on understanding the challenges facing organisations in adopting cloud computing, while the second questionnaire focused on understanding the information assurance practices of cloud vendors based on the results obtained from the first questionnaire survey.

This chapter provides a description of the survey undertaken, detailing the survey structure, respondents' profile, their geo-location, mode of conduct and results of the survey. A complete sample of the survey questions is provided in appendix A and B. After data collection, an analysis of the results was done on the questions having direct impact on the development of the roadmap. This chapter concludes by highlighting the key findings from the survey.

6.2 Audience

As the aim of the survey was to understand the challenges facing cloud computing adoption and the information assurance practices of cloud vendor in relation to cloud services, therefore, the targeted respondents were business managers such as CEO, CFO, VP, managers and information technology managers such as CTO, CIO. Business managers were preferable due to their position in organisation in procurement and funding of IT projects, while technical managers were preferred due to their understanding of technology and needs assessment for organisations. For the second survey which aimed at understanding information assurance practices, vendors were selected based on lists of best performers in the industry from publicly available sources such as CIO.com and focus. The criteria in vendor selection included vendor size, reputation and type of cloud service offered.

6.3 Methodology

The survey was conducted in late July to mid August and received 50% of responses from the industry. This was due to the facts that, during this time majority of them were in vacation. And this is the reason for the type of questionnaire distribution which was adopted by researchers.

The survey was based on two types of questionnaires, with two approaches. The first type of questionnaire focused on identifying the challenges facing cloud adoption as perceived by industry practitioners and was conducted using on-line surveys. The second type of questionnaire focused on understanding the information assurance practices of cloud vendors and was conducted offline.

The online survey was both effective and convenient. It was effective as it broadened the accessibility and reach of respondents, and convenient in that it did not require an immediate response from the respondent. It allowed for respondent to fill in the questionnaire at their own pace. For this survey to work, a mailing list for respondents was created, the survey posted online and invitations to participate were sent to the created mailing list.

The mailing list was created from expert and practitioners forum in the area of cloud computing of which the researcher is a member. These forums are the Cloud Security alliance, Cloud computing, and the cloud computing, VMware, Virtualisation and Enterprise 2.0 forums. After the creation of the mailing list, the questionnaire was posted online by the use of an online survey tool provided by surveyMonkey (http://www.surveymonkey.com/s/89JLHCD). This tool was useful to researchers as it allowed for response collection and provided capabilities for analysing the results. After posting the survey questions, invitations to participate on the survey were sent to the created mailing list. The invitation introduced the survey host, explained the aim of the survey and requested the respondent for their participation.

For the offline survey the researchers used publicly available information such as press releases, privacy policies, news articles and terms of service or contract terms in order to understand the information assurance practises of cloud vendors.

6.4 Questionnaire design

This section explains the structure of the survey by providing details of each question and its contribution to the research problem understanding and the development of the proposed roadmap. Just as a user manual explains the use and purpose of the device it accompanies, so this section explains the survey aim and purpose to avoid misunderstanding and confusion.

The online questionnaire had three sections. These are described as follows: The first section of the survey questionnaire aimed at understanding the respondent responsibility, nature of their organisation, their role in IT decision making, size of their organisation and the geographical location. This was important because personnel at different levels of management, with different level of involvement in IT decisions may have different understanding of technology and its impact to the organisation. Also as discussed in chapter 4, the geographical location of the company is affected legislation and compliance issues. The organisation size is also important as it affects how different systems and SLA are managed, as section 5.2, 5.4 and 5.5 have shown. This section was made up of question 1 to 3. The importance of these criteria in the proposed roadmap is alluded to in the analysis phase. In this phase the roadmap calls for an internal analysis of existing systems, security practices and policies, legal and compliance issues and how they may be affected by the move to cloud.

The second section of the survey questionnaire aimed at understanding the drivers for adoption, perceived appropriate cloud service deployment and delivery model and the type of IT or business processes that organisation are willing to outsource to cloud computing. This section was composed of question 4 to 6. As section 2.2.4 and 2.2.5, the understanding of these factors from the practitioner's point of view is crucial. This allowed the researchers to analyses any changes in practitioners understanding of cloud computing and its benefits. In the proposed roadmap the importance of this is shown in the planning phase where the organisation is to select and choose the appropriate cloud infrastructure and platform.

The third section of the survey is made up of question 7 through 10. In this section the survey aims at understanding the characteristics that are considered key to vendor selection, key concerns for vendor trustworthiness, and barriers to adopting cloud computing. As section 3.3.3, 4.4 and chapter 5, an understanding from the organisational perspective of

these factors was important in the development of the roadmap. This is shown in the roadmap phases such as planning, adoption, migration and management. The results from these questions also will help researchers to compare with results from previous researches and see if there are any changes from the organisations perspective.

The offline questionnaire has 7 questions which aim at understanding vendors' information security assurance in relation to privacy, disaster and business continuity, security practices and standards compliance, legal and compliance practices and SLAs management. As chapters 3, 4 and 5 have discussed these are among the greatest challenges that face cloud computing adoption from the organisation point of view. Therefore, an understanding of how vendors addresses these issues is crucial, as it helps in understanding why organisations are reluctant in adopting cloud computing and whether their perceived dangers of cloud computing are justifiable. These issues have been addressed in the proposed roadmap in the different phases.

6.5 Survey results analysis

In this section the analysis of the survey results is presented. The findings from the data collected and their findings are presented together with their analysis.

6.5.1 Online questionnaire survey results

In this survey, 50 invitations to participate in the survey were sent. The survey lasted for three weeks, and received a total of 25 responses, with 21 questionnaires fully completed. The response was high with participants from all over the world, with this response rate, useful information can be obtained.

- **Respondents by Job title**

The analysis of respondents by their job titles are as follows: IT management (Technical consultants/system integrator) 20%, business management (Consultant) 12%, IT management (CIO, CTO, CSO) 12%, IT management (Director/supervisor) 8%, business management (CEO, CFO) 8%, other IT staff 32%, other IT management staff 4%, other business management staff 4%. The cross section of respondents shows the level of reliability of the results and thus provides for good inputs for the design of the roadmap.

- **Respondents by role in IT decisions**

Based on the role of respondents in IT decision making the results are as follows: Evaluate/recommend vendor or solution 32%, determine IT needs 20% authorise purchase 16%, create IT strategy 16% and other 16%. These results show that the responds are personnel who know what their organisations needed in terms of IT resources, and have positions of influencing the final decisions.

- **Respondents by nature of organisation**

The nature of organisation was to determine whether the organisation was technical based or non-technical. The results obtained are as follows: Non-technical (education sector) 24%, technical (communications) 16%, technical (computer/networking) 16%, non-technical consultancy 8%, non-technical government 8%, technical e-commerce 4%, other technical 8% and other non technical 12%. The cross section of respondents from different industry increases the reliability of the results. This is because the variety of respondents from different industries removes bias to the survey results output.

- **Respondents by organisation size**

Base on the organisation size the results were as follows: employees between 1-99 (40%), 100 – 499 (32%), 500 - 999 (4%), 1000 – 4999 (12%) and above 5000 (12%). These results shows the level of complexity of adopting cloud computing that is to be expected as discussed in chapter 5.

- **Respondents by geo location**

The importance of geographical location of a company is crucial in such issues as legal and compliance (see section 4.3). The results to this question were: America (USA and Canada) 16%, Africa 48%, Europe 32%, Asia 16% and other part of the world 4%.

These responses forms part of the first section of the online questionnaire and relates to issues related to organisational challenges as discussed in chapter 5, legal and compliance issues discussed in chapter 4. The roadmap addresses these issues in its different phases.

The second section of the online survey yielded the following results:

- **Key drivers for adoption**

The results for on the different drivers for an organisation to consider cloud computing revealed that, the need for flexible IT resources was important with 68%, followed by resource optimisation at 44%, economies of scale 40%, security and resource diversification at 20% each and other reason which included back-up and efficiency for mobile and de-centralised workforce at 12%. These results show that there is a slight change in the reasons for adoption from costs to the need to increase efficiency and resource optimisation when compared to other research results. Figure 6-1 shows the summary of the results

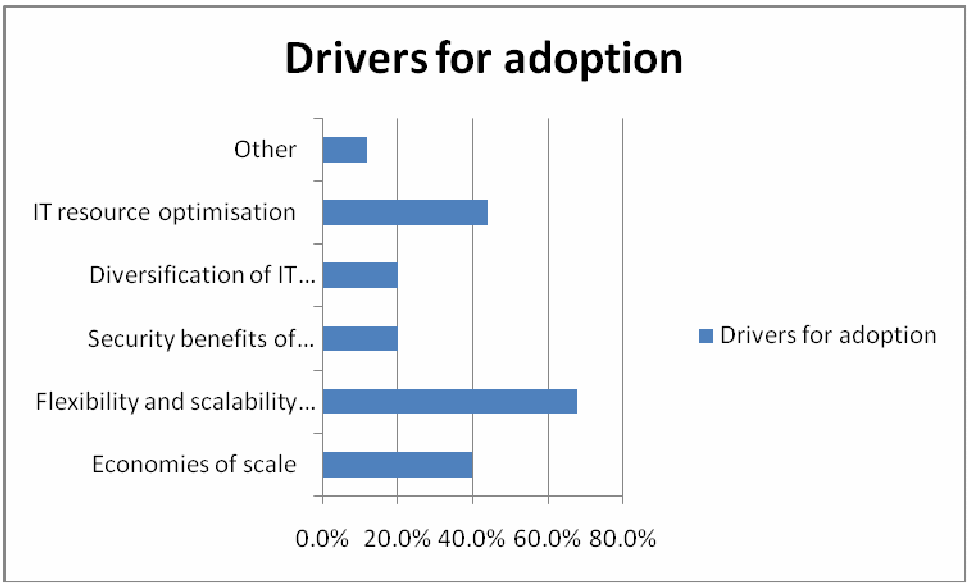

Figure 6.1: A summary of key drivers for adoption

- **Appropriate deployment and delivery model**

The results in this question showed that the most favourable cloud platform was SaaS with 60% followed by PaaS and IaaS with 20% each. These results suggest that organisations are more likely to use cloud applications and software such as CRM. For the delivery model the results showed that

- **IT resources or business process suitable for cloud computing**

For the type of IT and/or business processes that organisation are willing to outsource to the cloud the results showed that application development is more likely with 66% of the responses. CRM, sales and marketing and research and development both scored 33.3%, human resource management 19% while other such as e-mail, calendars and file storage had

9.5%. But in this question out of the 25 responses four questions were skipped. These results coincide with the conclusion drawn from the previous question on the application deployment model for cloud where SaaS received 60% as a favourable platform of choice.

Concerns identified in this section of the survey have been addressed in such sections as, section 2.2.4 and 3.3.2. The roadmap provides means of accessing these criterions for adopting cloud computing through its analysis and planning phases.

The third section of the survey aimed at understanding the key characteristics for vendor selection, vendor trustworthiness criteria and barriers to cloud adoption. The results for questions in this section were as follows:

- **Key characteristics for vendor selection**

Terms of service received 85.7% as an important criterion for vendor selection. This may be due to the fact that the terms of service determines a number of issues of concern such as security of applications and data, privacy and SLA. These results also confirm the security concerns as evidenced by our survey results and results from other research. Vendor reputation had 76.2%, vendor location 28.6% and this may be a results of many of the responses were from Africa where data protection legislation are not well developed (section 3.3). Vendors' size 19% and other which included pricing and privacy issues 9.5%. There were 4 skipped questions in this category. Figure 6-2 shows a summary of results.

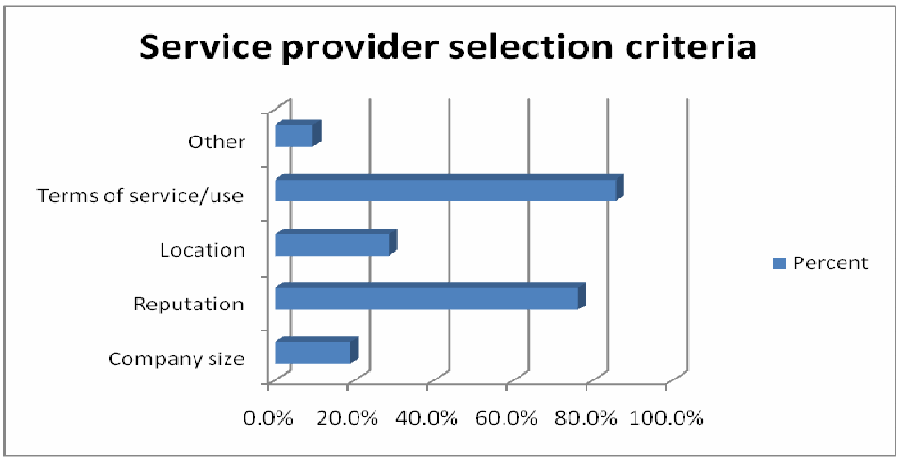

Figure 6.2: Service provider selection criteria

- **Key concerns for vendor trustworthiness**

Security practices with 90.5% was considered a very important aspect in determining trustworthiness, vendor reputation and terms of service had 47.6% each, compliance 42.9% information assurance practices 38.1% and other 4.8%. four questions were skipped. Figure 6-3 summarises the results.

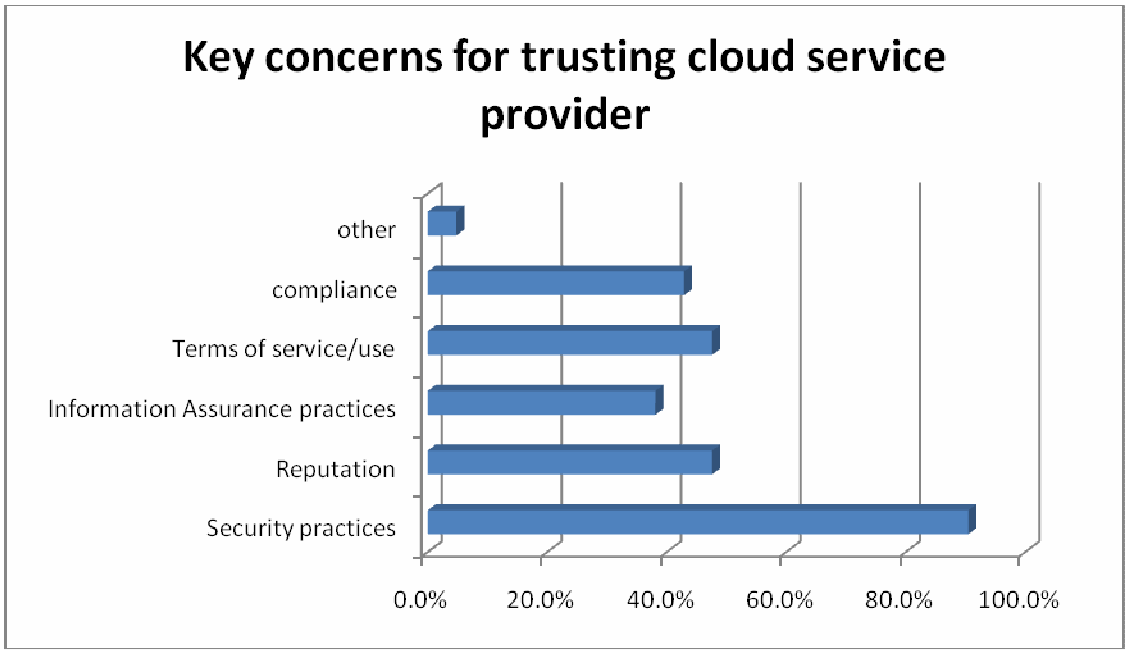

Figure 6.3: Key Trust concerns in adopting cloud computing

- **Indicators of vendors' trustworthiness**

Security practices of the vendor and business continuity and disaster recovery had 71.4% each followed by reputation at 57.1%, compliance 38.1% and other which included contract and terms of service at 9.5%. Four questions were not answered. Figure 6-4 shows a summary of results.

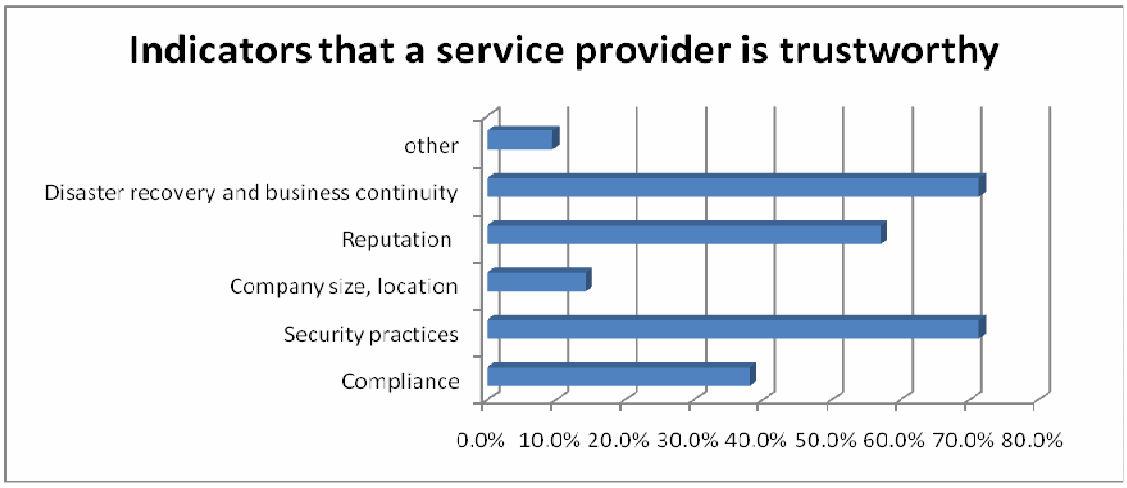

Figure 6.4: Indicators of service providers' trustworthiness

- **Barriers to cloud adoption**

Security concerns top the list with 71.4% followed by integration issues with 61.9%, regulatory and compliance and governance issues 42.9%, availability and performance 28.6% and other 4.8%.

These survey results show that security is still the main concern for organisation when considering cloud adoption. This survey found that security concerns had an average 71.4%, IDC 87.5% (IDC, 2009), SAVVIS 52% (SAVVIS, 2010). These results support the findings of section 3.2 which have identified a number of security issues facing organisation in cloud adoption. as for the reason to adopting cloud computing this survey have found that scalability and flexibility of resources are key. Figure 6-5 shows a summary of results.

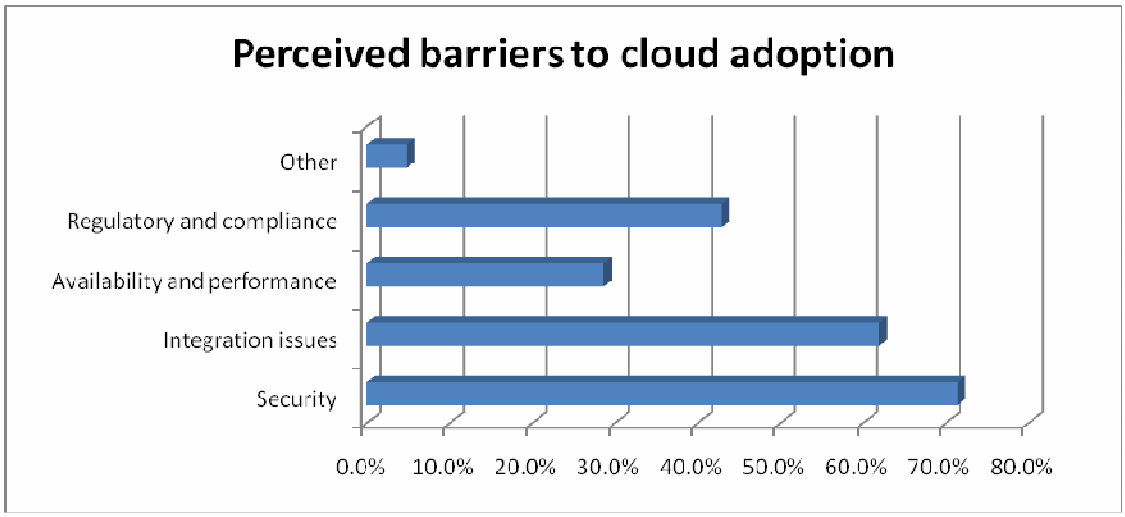

Figure 6.5: Barriers to cloud adoption

6.5.2 Offline questionnaire survey results

In this survey thirteen different cloud service providers were selected from the publicly available lists of best performers. The survey used publicly available information such as privacy policies of the service providers, press releases in order to understand the information assurance practices of the service providers. The survey focused on privacy, disaster recovery and business continuity, security practices, legal and compliance and SLA management. Table 6-1 shows a summary of cloud service providers and the platform of their cloud offering.

Service provider	Company size	Platform type
Microsoft SQL Azure	Large	IaaS
Google Docs	Large	SaaS
Google Apps Engine	Large	PaaS
Amazon	Large	SaaS
Salesforce.com	Large	SaaS
Microsoft office live	Large	SaaS
Oracle	Large	IaaS
Accenture	Large	PaaS
Rackspace	Small	IaaS
Cloud9Analytics	Small	SaaS
Cloudworks	Small	IaaS
Gogrid	Medium	PaaS
CloudAppy	Not available	PaaS

Table 6.1: Cloud Service providers and their attributes (Source: author)

The data collected from this offline survey of policy statements, press releases and other relevant documents including publicly available information from external sources, have shown the following:

- **Privacy:** From the survey findings, PaaS service providers puts comparatively not as much of emphasis on privacy as IaaS and SaaS service providers. This finding suggests that, most of the organisations that are involved with processing of individual data or personal information prefer cloud offering that assures them of full control of the infrastructure. This means that for such organisations PaaS and IaaS offer more suitable options. Another finding is that most of the SaaS services offer their services to individual customers'; as a result this imposes a responsibility of ensuring privacy of the individuals and their data (section 4.2.3 and 4.3.2).

- **Security practices and business integrity**: Findings in this category reveal that, as the cloud services goes high up the stack from IaaS to SaaS, emphasis on security and business integrity decreases. This may be due to lack of agreed upon cloud standards, lack of portability and interoperability. Another reason may be the potential of application lock-in (section 4.2.1 and 4.2.3). However, service providers make security a priority in their information and tend to offer business integrity as an added value service.

- **Legal and compliance issues:** the findings in this aspect show that, the responsibility for compliance to different legal requirements and standards is of the customer, while some service providers have started to have their services certified as exemplified by salesforce.com.

- **SLA management:** in SLA management most of the service providers promise 99.9% availability in their policy statements. However, in these policy statements they make it clear that if things go wrong they will only pay back the customer a certain amount of money for the failure to meet the SLA.

The findings in this survey confirms the perceived reluctance of organisation in adopting cloud computing. The findings show that most of the vendors do not provide for adequate security and compliance services that meets user or clients requirements. Section 4.2.4 and the roadmap address these issues by encouraging collaboration between client and vendor in the whole process of cloud adoption.

6.6 Summary of findings

In this section a summary of findings from the survey is given. Both the online and offline surveys have revealed a number of interesting facts. For example, depending on the nature of the respondent job and nature of the organisations, it was discovered that these two factors have effect on how the person perceives cloud computing, its drivers for adoption, barriers and trust issues. These are discussed briefly bellow.

- **Respondents profile**

The respondents for the online survey were from both technical and non-technical job roles and organisations. A summary of this is given in table 6-2. This table shows the different types of respondents and the nature of their job titles and organisations.

Nature of Job	**Nature of Organisation**	**Response count**	**Percentage**
IT management (Technical)	Technical	7	28%
IT management (Technical)	Non-Technical	12	48%
Business management (Non-technical)	Technical	5	20%
Business management (No-technical)	Non-technical	1	4%
Total		**25**	**100%**

Table 6.2: Respondents profile

This summary of respondents is has enabled the researchers to discover different perspectives and perception of drivers for adoption, barriers and trust issues as seen by these industry practitioners, tables 6-3 to 6-6 provides the findings on the drivers for adoption, trust issues of concern and barriers of adoption based on the respondent profile.

Nature of Job: Technical	**Response count out of 25**: 7
Nature of Organisation: Technical	**Percentage out of total responses**: 28%
Drivers for Adoption (Top 3)	**Response count for the category**
Flexibility and scalability for IT resources	5
Resource optimisation	2
Security benefit and economies of scale	2
Trust issues (Top 3)	
Disaster recovery and business continuity	5
Security practices	4
Compliance issues	2
Barriers to adoption (Top 3)	
Security concerns	6
Integration issues	3
Availability and performance	2

Table 6.3: Summary of key issues for respondents of the category-Job title: Technical and nature of Organisation: Technical

Nature of Job: Non-Technical	**Response count out of 25**: 12
Nature of organisation: Technical	**Percentage out of total responses:** 48%
Drivers for adoption (Top 3)	**Response count for the category**
Flexibility and scalability of IT resources	9
Resource optimisation	7
Economies of scale	6
Trust issues (Top 3)	
Security practices	10
Disaster recovery and business continuity	9
Service provider reputation	7
Barriers to adoption (Top 3)	
Regulatory, compliance and IT governance	7
Integration issues	6
Security issues	6

Table 6.4: Summary of key issues of the category-Job title: Non-Technical and Organisation nature: Technical

Nature of Job: Technical	**Response count out of 25**: 5
Nature of Organisation: Non-Technical	**Percentage out of total responses:** 20%
Drivers for adoption (Top 3)	**Response count for the category**
Flexibility and scalability of IT resources	3
Resource optimisation	2
Economies of scale	2
Trust issues (Top 3)	
Service provider reputation	3
Disaster recovery and business continuity	1
Compliance	1
Barriers for adoption (Top 3)	
Security issues	2
Integration issues	2
Regulatory, compliance and governance	1

Table 6.5: Summary of key issues of the category-Job title: Technical and Organisation nature: Non-technical

Nature of Job: Non-Technical	**Response count out of 25:** 1
Nature of Organisation: Non-Technical	**Percentage out of total responses:** 4%
Drivers for adoption (Top 3)	**Response count for the category**
Efficiency for mobile workforce	1
Trust issues (Top 3)	
Service provide size and location	1
Service provider reputation	1
Barriers for adoption (Top 3)	
Integration issues	1
Security concerns	1

Table 6.6: Summary of key issues of the category-Job title: Non-Technical and nature of Organisation: Non-Technical

- **Drivers for adoption**

Findings from our research have revealed that, most of the organisations that have adopted cloud computing are currently using cloud services at upper stack of the platform as compared to the lower stack (section 6.5.2). However, majority of cloud services are still individuals as opposed to organisations. The biggest driver for cloud adoption for most organisation has been found to be the need for flexible and scalable IT resources (see tables 6-3 to 6-6), followed by the need for resource optimisation. The findings suggest that costs is not the biggest drive by itself but rather through the other benefits of adopting cloud computing costs may be reduced.

- **Barriers to adoption**

The research findings have shown that personnel with technical understanding of technology as well as those without all consider security to be the most significant factor in cloud adoption as pointed out in section 4.2.2 and 4.2.3. This may be due to the emphasis placed on security by technical personnel in the organisation infrastructure as well as the security awareness programs and trainings. The second most important barrier identified was integration issues with existing systems and application. This was more a concern for organisations that were not technical in nature (see tables 6-3 to 6-4).

- **Trust**

The findings on this issues as it relates to cloud adoption found that security practices and disaster recovery and business continuity were important from both technical and non-technical organisation and personnel. Tables 6-3 to 6-4 provide a summarised view.

Other findings are that based on the country of respondents issues related to regulatory and compliance was affected. While respondents from Europe, America and Asia considered these issues important those from Africa had a different view. Therefore it will be interesting to study and find out if such difference are due to lack of legislation in most African countries related to data protection and privacy or is dependent on the nature and the size of the organisation and whether it business is global.

In this dissertation three research questions were answered. The first question was related in identifying the key barriers to cloud computing adoption, the second dealt in seeking to understand if it is possible for customer and service provider to collaborate for successful adoption of cloud computing. These two questions have been addressed so far. Chapters 3, 4 and 5 have identified the key barriers to adoption and this survey results have confirmed and prioritised those barriers based on the findings. The possibility of customer and service provider collaboration has been addressed in section 4.2.4 and is also emphasised in the roadmap (chapter 7). The last question concerned itself with identifying how organisation can address the challenges facing cloud adoption and how to successfully adopt cloud computing. The answer to this question is the proposed roadmap which is discussed in chapter 7 and a worked example of the viability of the solution is provided in chapter 8. It was also, hypothesised that by the use of the proposed roadmap technical managers as well as business managers will have a better understanding of the key issues involved in cloud computing and a tool to guide the process of adopting cloud computing. The hypothesis is tested in chapter 8 and its results are discussed.

6.7 conclusion

This chapter discussed the survey conducted and its results analysis. The survey audience was described in section 6.2 which included both IT and business managers. The survey methodology which employed the use of both offline and online questionnaire was given in section 6.3 while the survey design was presented in section 6.4. The survey results were

discussed in section 6.5 and summary of the survey findings was given in section 6.6. Chapter 7 describes the proposed roadmap and its evaluation framework.

7. ROADMAP AND EVALUATION FRAMEWORK

7.1 introduction

As the previous chapters have demonstrated, a successful cloud computing adoption must focus on the areas of trust, security, legal and compliance, and organisational issues. This chapter integrates the critical issues from the previous chapters into a roadmap for successful cloud computing adoption project. Managers can use this roadmap to address strategic issues at each stage of the project lifecycle. The roadmap is called ROCCA (Roadmap for Cloud Computing Adoption). Also included is the ROCCA Achievement Framework (RAF) which establishes the level of adherence to the proposals in the roadmap.

7.2 ROCCA (Roadmap for Cloud Computing Adoption)

The necessity of collaboration between customers and service providers cannot be overstated.

Figure 7-1 shows the proposed cloud computing adoption roadmap. The roadmap proposes five (5) phases in the adoption of cloud computing project. These are: analysis, planning, adoption, migration and management.

The framework works as follows: in the analysis phase, the analysts works with users and conducts an analysis of the existing systems, applications and business processes, by using tools such as SWOT analysis, PESTLE analysis in order to ascertain the directions, an analysis of security, legal and compliance issues, usability and accessibility issues, and analysis of impact to organisation structure, and culture is done. This phase identifies the strengths and weakness of the existing systems, applications and business process, the impact of moving to cloud and identifies possible candidates for migration to cloud. The planning phase deals with benchmarking, choosing the platforms for deployment, the cloud infrastructure, finance plan, security, legal and compliance plan and the roll-out plan for the adoption project. This phase sets the objectives and the direction for the adoption of cloud computing. In the adoption phase the analyst and the project team works on application integration with cloud platforms and infrastructure, outsourcing strategies, works on SLAs, customer service management, security policies, legal and compliance management and a

contract with vendor is developed and signed. This phase sets the stage for migration of the selected applications and systems to the cloud.

The migration phase ensures that application and data migration are carried out as specified in the roll-out plan which was developed in the planning phase. The phase also ensures the availability of users support in the whole process of migrating to the cloud and monitors and control the migration. In the last phase, that is management phase the project team works to ensure contracts are properly managed and that the project is signed off. Best practices and lessons learnt are documented, technical support is ensured for continual support of the systems and users and a review of the whole project is done. This roadmap is generic and is based on research carried out in chapters 2, 3, 4, 5 and 6, and therefore can be applied to the domain of cloud computing.

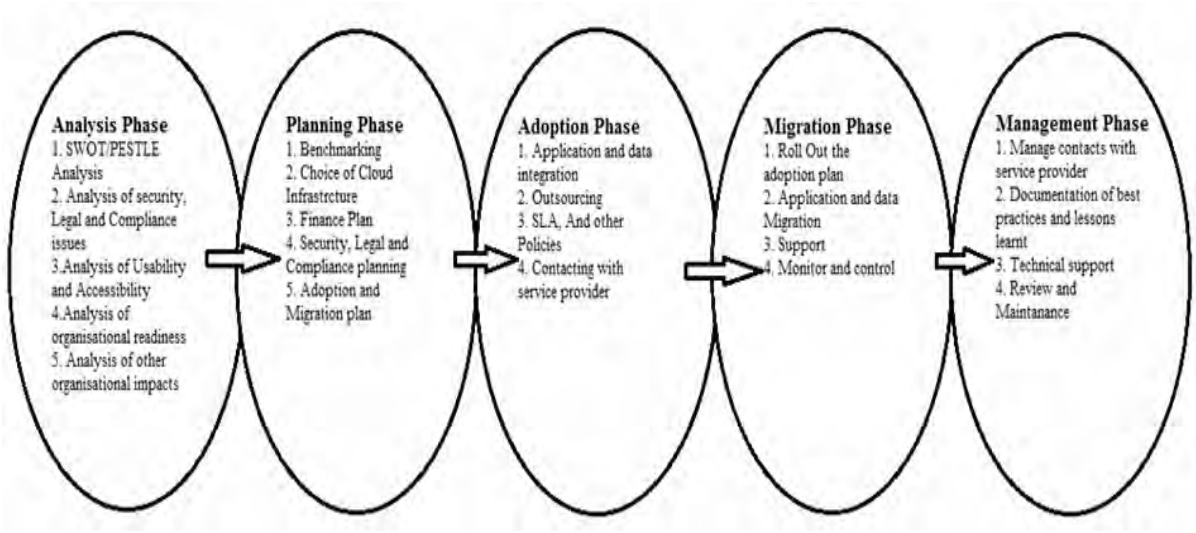

Figure 7.1: Cloud computing Adoption strategies (Author)

Table 7-1 provides a generalised summary of the main challenges that have been identified and where in the roadmap they are addresses.

Challenge	Chapter	Phase
Trust	3	Analysis, Planning and migration, Adoption
Security	4	Analysis, planning, Migration
Legal and Compliance	4	Analysis, planning
Organisational	5	Analysis, Planning, Migration and Adoption

Table 7.1: A summary of challenges and the respective phase that address them (Source: author)

An example of how the roadmap can be used is given. Suppose and organisation is seeking to adopt cloud computing but they are unsure of how much it will cost and what will be the impact to the organisation IT budgeting and procurement procedures. In the analysis phase tools such as SWOT can be used to identify the current state of the IT financial status and the IT procurement procedure, then from the analysis the impact of cloud computing to the existing procedures is done using a tools such as PESTLE analysis or other tools that a familiar to the organisation. Cost benefit analysis is also conducted to determine whether the move will have any positive financial implications to the organisation. In the planning phase any changes that are expected as identified in the analysis phase are communicated to the affected parties. Based on the analysis a financial plan is made. For example if the organisation uses a chargeback mechanism for funding its IT usage in the organisation, then a plan need to be made and a decision as to how individual departments or section are going to use cloud services. This decision and plan will have impact in the procurement procedure for IT resources. One of the options may be to continue with chargeback internally while using corporate budget in procuring cloud services. This will be dependent on the analysis results and the perceived impact. The result from the planning phase will be basis for the adoption phase, and the drafting of internal and external contracts for the use of cloud services, SLAs and other user policies. In the migration phase proper controls and checks are developed and set to ensure that the financial and procurement policies and plan are being followed while the management phase will document all the lessons learnt and best practices for future references and projects.

Phase 1: Analysis

As with all software projects, the initial stage is understanding users' requirements in order to determine whether the project is feasible. It is at this stage that the initial requirements, feasibility, project scope, costs and initial plan will be developed.

During this phase of the project, the business case is developed. Thought should be given to how the existing systems strengths and opportunities can be maximised, weaknesses and threats minimised (section 5.3), the impact to organisation culture, processes, and structure minimised, and the effect to SLAs (section 5.2 and 5.5), how return on investment and costs to adopting cloud computing can be managed (section 5.6) and the usability and access to resources will be assured and maintained (section 5.4 and 5.5). Also the impact to organisational security policies, standards and legal and compliance issues (section 4.3.2, 4.2 and 4.3). in order to analyse the strengths, weakness, opportunities and threats of existing systems a SWOT matrix (Swinton, 2004) is useful, in accessing the organisational impact of moving to the cloud the PESTLE matrix developed by Associates is invaluable (Associates, 2003). Also the organisation may use tools that are familiar within the organisation. Also in this phase candidate systems and or application for cloud migration are identified. Table 7-2 summarises the issues that are addressed by the analysis phase.

Issue	Section
Trust	Chapter 3
Security	4.2
Legal and Compliance	4.3
Organisational change	5.2
Governance and risk management	5.3
SLA Management	5.5
The economics of cloud computing	5.6

Table 7.2: summary of issues addressed in analysis phase (Source: author)

Phase 2: Planning

In this phase benchmarks for security, legal and compliance issues identified in the analysis phase are set. The benchmarks will reflect the internal organisational best practices, policies and standards to industry standards and best practices (section 4.2.4) and how these can be achieved when moving to the cloud. The benchmarks also will reflect the legal and compliance best practices that need to be maintained and achieved in the cloud environment (section 4.3.1 and 4.3.3). The selection of cloud computing platform and infrastructure suitable for the organisations' systems and applications to be moved to the cloud is done (section 2.2.3, 2.2.4 and 2.2.5). Financing and cost management plan is developed and how costs will be managed. The method or model of payment is decided upon and how this is to

be managed internally (section 5.6). The plan on how to ensure security compliance, legal and compliance to industry standards and regulation is laid down (section 4.2.4 and 4.3).

In preparing the adoption or roll-out plan it is important at this stage to decide whether prototyping of the cloud services will be used and whether there will be pilot projects before full roll-out and identifying risks and how they are to be mitigated (Section 5.3). Table 7-3 summarises the issues addressed in the planning phase.

Issue	**section**
Technology	2.2.3
Service and deployment models	2.2.4
Drivers and benefits of adoption	2.2.5
Standards and best practices	4.2.4
Legal and compliance issues	4.3
Legal challenges	4.3.2
Compliance issues	4.3.3
Governance and risk management	5.3
The economics of cloud computing	5.6

Table 7.3: summary of issues addressed in the planning phase (Source: author)

Phase 3: Adoption

This phase is a preparation phase for the actual migration of systems and/or applications selected to the cloud platform and infrastructure of choice. In this phase systems/ application integration is done to ensure that the candidate applications will be able to function with the internal applications that are not migrated to the cloud and also with the cloud infrastructure of choice (section 5.4 and 5.5). Outsourcing strategies are decided upon and the benchmarks developed in the planning phase are used to measure vendor ability to provide service that will not affect the organisation service delivery and business. As shown in section 4.2.4 and section 5.5, collaboration with vendors is crucial in establishing SLA agreements and different security policies and best practices to ensure compliance and trust. The last thing in this phase is contract development and signing that meets the user requirements for using cloud services. Table 7-4 summarises the different issues that the adoption phase addresses.

Issue	**section**
Trust	2.3.2
Standards and best practices	3.2.4
Systems and application migration	4.4
SLA management	4.5

Table 7.4: A summary of issues addressed in the Adoption phase (Source: author)

Phase 4: Migration

At this point the preparation for migrating to the cloud concludes and migration can proceed. Either the project can be discarded or enhanced to meet the user requirements. Given the outcomes from the three previous phases, the roll-out plan can be put into practice. Applications and data migration can proceed. Support to users during the migration process is provided, and the monitoring and control of the project is maintained to ensure successful migration. Table 7-5 summarised the different issues facing cloud adoption that the migration phase addresses.

Issue	section
Security challenges in cloud computing	4.2.1
Sources of perceived threats	4.2.3
Standards and best practices	4.2.4
Legal challenges	4.3.2
compliance	4.3.3
Governance and risk management	5.3
SLA management	5.4
The economics of cloud computing	5.5

Table 7.5: A summary of issues addressed in the Migration phase (Source: author)

Phase 5: Management

The project now should be fully operational in the cloud; however contract and vendor management, testing and maintenance, user support and review should be ongoing for several months subsequent to launch. The system metrics or benchmarks developed and set in phase 2 can be used as indicators of project success and should be monitored (section 4.2, 4.2, 5.3, 5.5 and 5.6). Security standards compliance, SLAs, legal and compliance issues, IT governance best practices and cost management are desirable metrics.

Also documentation of lessons learnt and best practices during the project should be documented and communicated to all stakeholders. Table 7-6 provides a summary of different issues addressed by management phase.

Issue	Section
Cloud Adoption	The whole project

Table 7.6: A summary of issues addressed in the Management phase (Source: author)

7.3 RAF (ROCCA Achievement Framework)

Section 7.2 provided a high level roadmap for cloud computing adoption project. This section proposes a framework, which can be used to establish achievement level based on the proposed roadmap. Therefore, the framework will be referred to as ROCCA achievement framework (RAF). The primary objective of the framework is as a tool for analysing projects carried out based on the roadmap. The use of the framework should be helpful in determining how closely the roadmap was followed in adopting cloud computing. As the roadmap is based on research into challenges and best practices in adopting cloud computing (chapters 2, 3, 4, 5 and 6), a project with high scores in the framework is more likely to succeed.

The framework is divided into five sections, corresponding to the five phases of the cloud computing adoption roadmap proposed in section 7.2. Each section contains a series of questions, which should be answered on a scale of 1 to 5. 1 indicates an unfavourable response to the question and 5 a strongly favourable response. Each response is then multiplied by a specific project weighing factor. The weights to be applied are decided upon in advance by the project management team. Different projects may have different weights based on the perceived impacts of the response to the overall projects' success. SLA for example might have a lower weighting than compliance for a non critical application. However if the application is critical SLA might be rated higher.

However, leaving this weighting process to project teams lead to the problem of possible subjectivity in assigning weights. However, based on this research findings from its literature review (chapters 2 to 5) and survey results, it is suggested that all questions related to security, legal and compliance be given a weight not less than .8 and a maximum of 1. Those related to requirements understanding a weighting not less than .5, system performance .7, finance .7 and SLAs .6. The various sections of RAF framework are outlined in tables 6-7 to 6-11.

Phase 1: Analysis			
Question	**Weight**	**Response**	**Score**
1. Have the initial project requirements been identified and defined?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
2. Has the analysis of internal systems and application been done? Were proper analysis tools used?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
3. Have security, legal and compliance issues for migrating to cloud analysed?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
4. Have the risks and benefits of outsourcing to cloud been analysed?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
5. Is the impact of moving to cloud to different stakeholders been analysed**?**		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
6. Has the financial implications been analysed?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
7. Are the candidate applications/systems been identified?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
Weighted Total			

Table 7.7: RAF - Analysis phase (Source: author)

Phase 2: Planning			
Question	**Weight**	**Response**	**Score**
1. Are systems and application metrics known?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
2. Have benchmarks for candidate applications/systems set?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
3. Have the cloud platform and infrastructure been selected based on the metrics?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
4. Is the cost management and finance plan developed? Does it address the mode of payment?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
5. Is the plan for security, legal and compliance management feasible?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	

6. Were vendor involved in developing the security. Legal and compliance plan?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
7. Does the roll-out plan details and specify the candidate systems? Is prototyping or trial service going to be used before actual migration?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
Weighted Total			

Table 7.8: RAF - Planning phase (Source: author)

Phase 3: Adoption			
Question	**Weight**	**Response**	**Score**
1. Are prototypes or trial service to be used to ensure application integration?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
2. Are outsourcing strategies compliant with procurement procedures?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
3. Have SLA, security policies and IT governance procedures agreed upon with vendor?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
4. Is the contract written in a manner that guarantees the client value for money?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
Weighted Total			

Table 7.9: RAF - Adoption phase (Source: author)

Phase 4: Migration			
Question	**Weight**	**Response**	**Score**
1. Is the roll-out plan comprehensive and detailed enough?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
2. Are users affected by the migration aware of the changes?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
3. Are application/data for migration critical to the organisation?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
4. are user support and control and monitoring mechanism in place?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
Weighted Total			

Table 7.10: RAF - Migration phase (Source: author)

Phase 5: Management			
Question	**Weight**	**Response**	**Score**
1. are contract and vendor management done appropriately?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
2. has the project been signed off?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
3. have the lessons learnt and best practices been documented?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
4. have technical support been established or outsourced?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
5. is testing and maintenance plan in place for the first few months after launching?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
6. are application metrics and data being collected, analysed and used to enhance project success?		☐ ☐ ☐ ☐ ☐ 1 2 3 4 5	
Weighted Total			

Table 7.11: Management phase (Source: author)

Weighted totals from table 7-7 to table 7-11 are used as input score to table 7-12. This table provides a means for weighing each phase based on the phase impact on the overall projects' success. The weights for each phase should be determined in advance by the project management team based on the overall impact of the phase to the particular project.

Project Phase Totals			
	Phase	**Weight**	**Score**
1	Analysis		
2	Planning		
3	Adoption		
4	Migration		
5	Management		
Overall Total			

Table 7.12: RAF - Project phase totals (Source: author)

7.4 Conclusion

This chapter proposed ROCCA (Roadmap for Cloud Computing Adoption) and RAF (ROCCA Achievement Framework). ROCCA proposes a five-phase process. In the analysis phase strengths and weaknesses, opportunities and threats to organisations systems,

applications and business process are identifies, legal, security and compliances policies and risks are identified, usability and accessibility risks and impact of moving ot cloud to the organisation culture, politics and structure are analysed. The monetary implications of moving to the cloud are assessed and candidate applications and or systems are identified. In the planning phase, benchmarks are set for the project, the cloud infrastructure and platform are selected, the financing plan is developed, security, legal and compliance plan is developed and the roll-out plan for adoption is created.

The adoption phase ensures application and systems integration with selected cloud platform and infrastructure for candidate systems and applications, outsourcing strategy are developed and put in place, SLA and policies for cloud service use are developed and put in place, the contact with cloud vendor is developed and agreed upon. In the migration phase the roll-out plan is reviewed and implemented, application and system migration to cloud is carried out, support channels are created and support is offered to users during the migration phase, monitoring and control of the migration of data and application is conducted to ensure success. The management phase ensure project sign-off, contract management with vendor, documents best practices and lessons learnt, technical support management and training of users, also review of the project is conducted as this is an on-going phase of the project after the actual migration.

The ROCCA achievement framework's (RAF) goal is as a tool for analysing the success of cloud computing adoption project based on the proposed roadmap. By using the framework project managers should be able to establish how closely the roadmap was followed. Based on the framework a project with high scores has a higher probability of success.

The framework has been divided into five phases of cloud computing adoption project. Each section is composed of a series of questions, with their corresponding weights. The weights to be applied are to be decided by the project management team in advance based on the perceived impact of the phase on the overall project success. Different projects will have to weigh each of these weights differently.

The joint usage of the ROCCA and RAF in a cloud computing adoption project should result into an integrated project plan and evaluation framework, minimising risks and

increasing the probability of projects' success. Chapter 8 presents a walkthrough evaluating the proposed roadmap and its framework.

8. ROCCA ACHIEVEMENT FRAMEWORK (RAF) WALKTHROUGH

8.1 Introduction

This chapter presents a walkthrough of a case study provided by Mr. Wawila Mwazembe of Dar411. Mr. Mwazembe has experience as system administrator, It consultant and project supervisor for three years and is currently the Chief Information officer of Dar411.

8.2 Project background

Dar411 is a private owned company that trades in the media and entertainment industry. The company is headquartered in Dar es salaam, Tanzania and serves the East Africa community.

The company is in the process of overhauling its IT infrastructure and is working on developing a cloud solution. The reason behind this is the need to increase performance, scalability and utilisation of resources. Another reason is the need to reduce running and operation costs. The project is substantial to the company, it the company intends to utilise its existing IT skills and resources in collaboration with service provider in developing the cloud solution. The solution that the company seeks to develop is based on the SaaS platform and is to be a private cloud hosted by a trusted third party.

8.3 RAF walkthrough

Table 8-1 to 8-5 represents the responses to each question for the project outlined in section 7.2. The weighing factors proposed in the ROCCA Achievement Framework (RAF), were decided upon by Mr. Mwazembe and represent the perceived importance of the outcome to that particular question in relation to the overall success of the project.

Table 8-6 represents the totals of each phase of the project as obtained from the weighted totals in tables 8-1 to 8-5. The table also provides the total for the entire project. As is evidenced by table 8-6, the project scores 66.6. For this number to be a truly useful indicator for achievement, it needs to be compared with totals derived from a range of similar successful and unsuccessful projects. This is left for a future research. The following

tables, table 8-1 to 8-6, represent the results of using the framework as worked out by Mr. Mwazembe of Dar411.

Phase 1: Analysis			
Question	**Weight**	**Response**	**Score**
1. Have the initial project requirements been identified and defined?	1	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	4
2. Has the analysis of internal systems and application been done? Were proper analysis tools used?	.9	☐ ☐ ☐ ☐ ☒ 1 2 3 4 5	4.5
3. Have security, legal and compliance issues for migrating to cloud analysed?	1	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	4
4. Have the risks and benefits of outsourcing to cloud been analysed?	.9	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	3.6
5. Is the impact of moving to cloud to different stakeholders been analysed**?**	.8	☐ ☐ ☒ ☐ ☐ 1 2 3 4 5	2.4
6. Has the financial implications been analysed?	1	☐ ☐ ☒ ☐ ☐ 1 2 3 4 5	3
7. Are the candidate applications/systems been identified?	.5	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	2
Weighted Total			23.5

Table 8.1: Analysis phase worked out example (Source: author)

The following are the observation and comments from Mr. Mwazembe on the analysis phase.

- The novelty of cloud computing has necessitated an intensive analysis and requirement gathering. This was considered important since cloud computing is still in its early stages.
- The organisational impacts to culture, politics and work processes and procedures were carefully assessed and analysed.
- The procurement and financial implications of cloud computing were closely analysed.

- Mr. Mwazembe felt that, the use of analysis tools which are familiar to many business mangers and technical personnel in the analysis phase was crucial in building trust towards cloud computing adoption.

Phase 2: Planning			
Question	**Weight**	**Response**	**Score**
1. Are systems and application metrics known?	.8	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	3.2
2. Have benchmarks for candidate applications/systems set?	1	☐ ☐ ☒ ☐ ☐ 1 2 3 4 5	3
3. Have the cloud platform and infrastructure been selected based on the metrics?	.8	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	3.2
4. Is the cost management and finance plan developed? Does it address the mode of payment?	.9	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	3.6
5. Is the plan for security, legal and compliance management feasible?	1	☐ ☐ ☒ ☐ ☐ 1 2 3 4 5	3
6. Were vendor involved in developing the security. Legal and compliance plan?	.7	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	2.8
7. Does the roll-out plan details and specify the candidate systems? Is prototyping or trial service going to be used before actual migration?	.9	☐ ☐ ☒ ☐ ☐ 1 2 3 4 5	2.7
Weighted Total			20.8

Table 8.2: Planning phase worked example (Source: author)

The following are the observation and comments from Mr. Mwazembe on the planning phase.

- The use of benchmarks based on organisation's familiar benchmarking tools and benchmarks for the planning phase was important. This allowed for use of existing systems benchmarks for planning for migration to cloud.
- The benchmarks also were an important aspect in planning for performance measures for systems and applications that were moved to the cloud.
- Mr. Mwazembe felt that, benchmarks are a good starting point in selecting and monitoring applications for migration to the cloud. Also for selecting appropriate cloud infrastructure and service provider.

- The planning phase was seen as a crucial phase in the perceived success level of the overall project. This is because the phase interprets the results of analysis phase into plans for adoption and selection of cloud infrastructure and service provider.

Phase 3: Adoption			
Question	**Weight**	**Response**	**Score**
1. Are prototypes or trial service to be used to ensure application integration?	.7	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	2.8
2. Are outsourcing strategies compliant with procurement procedures?	.8	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	3.2
3. Have SLA, security policies and IT governance procedures agreed upon with vendor?	1	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	4
4. Is the contract written in a manner that guarantees the client value for money?	.9	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	3.6
Weighted Total			13.6

Table 8.3: Adoption phase worked example (Source: author)

The following are the observation and comments from Mr. Mwazembe on the adoption phase.

- While in general this phase is important, the previous two phases are key in ensuring effective collaboration with vendor.
- This phase is important in setting out the contract terms and agreement on different issues identified in the analysis and planning phases.
- Mr. Mwazembe sees this phases' success being dependent on proper analysis and planning which are results of the previous two phases.

Phase 4: Migration			
Question	**Weight**	**Response**	**Score**
1. Is the roll-out plan comprehensive and detailed enough?	1	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	4
2. Are users affected by the migration aware of the changes?	1	☐ ☐ ☒ ☐ ☐ 1 2 3 4 5	3
3. Are application/data for migration critical to the organisation?	1	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	4

4. Are user support and control and monitoring mechanism in place?	.8	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	3.2
Weighted Total			14.2

Table 8.4: Migration phase worked example (Source: author)

The following are the observation and comments from Mr. Mwazembe on the migration phase.

- This phase is more of an implementation phase where the candidate applications and systems are moved to the cloud.
- The importance of this phase was in its emphasis on user involvement and the identification of the criticality of affected data to the business.
- Mr. Mwazembe felt that the involvement of users in this phase as critical in addressing issues related to resistance to change and addressing the social-technical changes that are the result of adopting cloud computing.
- The requirement of the phase to ensure user support and monitoring control were seen as important indicators towards the success of adoption and take-off of the project after successful migration to the cloud.

Phase 5: Management			
Question	**Weight**	**Response**	**Score**
1. Are contract and vendor management done appropriately?	1	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	4
2. Has the project been signed off?	.8	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	3.2
3. Have the lessons learnt and best practices been documented?	.9	☐ ☐ ☐ ☒ ☐ 1 2 3 4 5	3.6
4. Have technical support been established or outsourced?	.9	☐ ☐ ☐ ☐ ☒ 1 2 3 4 5	4.5
5. Is testing and maintenance plan in place for the first few months after launching?	1	☐ ☐ ☐ ☐ ☒ 1 2 3 4 5	5
6. Are application metrics and data being collected, analysed and used to enhance project success?	1	☐ ☐ ☐ ☐ ☒ 1 2 3 4 5	5
Weighted Total			25.3

Table 8.5: Management phase worked example (Source: author)

The following are the observation and comments from Mr. Mwazembe on the management phase.

- This phase was deemed important for a phased cloud adoption project as it requires documentation of the lessons learnt and best practices. This documentation is crucial for the success of future projects or projects that are carried out in phases.

Table 8-6 provides the weighted totals from the case study and walkthrough provided by Mr. Mwazembe.

Project Phase Totals			
	Phase	**Weight**	**Score**
1	Analysis	.8	23.5
2	Planning	.8	20.3
3	Adoption	.5	13.6
4	Migration	.5	14.2
5	Management	.7	25.3
Overall Total			66.6

Table 8.6: Project phase totals worked example (Source: author)

8.4 Evaluation of the proposed roadmap and framework

Mr. Wawila Mwazembe reviewed the roadmap and framework and found that they.... he agreed/disagreed with the five phases and indicated that he found the framework to be useful and effective tool for analysing cloud adoption projects. The process of using the framework in real project highlighted a number of issues. These issues identify the strengths and weaknesses in the proposed roadmap and framework, and highlighted potential areas for improvements. These issues are summarised as follows:

Planning and analysis

The author's research has emphasised collaboration and use of best practices and standards for successful cloud adoption projects (section 4.2.4; 5.2; 5.3 and 5.5). And the roadmap emphasises proper analysis and planning for cloud adoption projects. Mr. Mwazembe has indicated that, this however does have great impact on the success of cloud adoption projects. However he pointed out that these two phases a very useful for organisations that have IT infrastructure in place and are seeking adoption of cloud computing. Thus he

suggests that a different roadmap be developed to help start-up companies that have no prior existing infrastructure.

Collaboration between customers and service providers

This is another issue that the author's research has emphasised upon, but it was not clearly addressed in the roadmap and the mechanisms for collaboration were not clearly suggested. Mr. Mwazembe contented that this recommendation applies more to large organisation with stringent legal and security compliance requirements than with small organisation with less such requirements. Thus, this factor needs to be clearly incorporated in the roadmap and its framework.

Adding strategic focus to the roadmap

The proposed roadmap was divided into five (5) phases and its framework into six (6) sections five of which covers the phases in the roadmap and a final section provides an aggregate of the scores from the five phases of the roadmap. This aggregate score provides the scores for each of the 28 issues identified and all the five phases and for the project as a whole. The analysis of the case study has shown that a further analysis based on the strategic focus would have been useful. This calls for a different or reworked framework that categorise issues by strategic focus rather than by project phases. The categorisation of issues could be for example as technical, legal, personnel, financial and organisational. This re-categorisation would help to analyse similar projects to the one presented, which may have been successful in some areas, but failed in others.

Based on these findings, it is proposed that future work on the roadmap and framework should include a number of case studies in order to benchmark projects analysed using the framework. This corpus of case studies should include both successful and unsuccessful projects, which are projects that encountered difficulties in various stages. This would result in improved applicability of the framework. Future work should also include reassessment of the several issues proposed, such as planning and analysis phase that addresses the needs of newly established organisations, re-categorisation of the framework issues based on strategic focus. Re-focusing the framework focus towards enterprises that seek to completely outsource their IT infrastructure to the cloud would prove valuable.

The results and recommendations from this walkthrough support the hypothesis put forward. For this research project it was hypothesised that: by using the developed roadmap, business and IT managers will have a better understanding of the different key issues facing cloud adoption and will provide them with a tool to guide the process of cloud computing adoption. The case study walkthrough have demonstrated that the roadmap is a useful tool for understanding different issues and as a tool for guiding adoption of cloud computing solutions to both technical and business managers.

8.5 Conclusion

This chapter presented a walkthrough of a case study provided by Mr. Wawila Mwazembe of Dar411.

The project described involved development of cloud computing solution for the company. While the project was a success it is still very early to evaluate its success from a business point of view.

The walkthrough is an illustration of how RAF can be used in a project. It presents responses to all the questions proposed in the framework. The responses refer to the case study described. For each project phase, a weighted total is provided and an overall total for the project represents the degree by which the project adhered to the proposals in the ROCCA. Chapter 9 presents the research conclusions.

9. CONCLUSION

9.1 Introduction

This chapter reviews the dissertation and research carried out in its production. In this research project three questions were answered and a hypothesis evaluated. The questions were: 1. what are the key challenges facing cloud adoption? 2. Is it possible for customer and cloud service providers to collaborate for a successful cloud computing adoption project? And the last question was: can a roadmap to address the challenges facing cloud computing adoption be developed? These questions have been answered in chapters 2, 3, 4 and 5 while chapters 6 and 7 addressed the last question. The hypothesis for this research was: that the developed roadmap would enable technical managers and business mangers to understand key issues facing cloud adoption and act as a guiding tool towards successful adoption. The hypothesis has been evaluated in chapter 8 through a case study and walkthrough provide by Mr. Mwazembe.

The research was critically evaluated and recommendations drawn from the analysis. Whilst chapter 6 placed all the research recommendations from the three preceding chapters in the context of a roadmap and an associated framework, this chapter set apart 4 high level areas of focus. These recommendations are important to successful cloud computing adoption projects. The recommendations are:

- Collaboration between customers and cloud service providers.
- The use of security and IT governance best practices migrating to clouds
- Analysis and planning should form the basis of any cloud adoption project
- Organisational factors (in particular the impacts of migrating to the cloud on culture, politics and work processes) are critical to success
- Projects deployed based on best practices and agreed upon security and compliance issues between customer and service provider should result in long term benefits to the organisation.

The chapter also discusses future research areas. As the discipline of cloud computing is still immature, the scope for future research is wide. Some of the suggestions outlined in this chapter include the impact of cloud computing to the social-technical aspect of the organisation.

9.2 Research Definition & Research Overview

Successful adoption of cloud computing is key for realisation of benefits promised by cloud computing environment. As organisations are faced with the need for high processing capabilities, large storage capabilities, IT resource scalability and high availability, at the lowest possible cost, cloud computing becomes an attractive alternative. However, the nature of cloud computing pose challenges to organisation as they consider adopting it. Issues such as security, legal and regulatory compliance become more prevalent.

The aim of the research project was to investigate the challenges facing cloud computing adoption and synthesise a roadmap which will provide organisations with guidelines for successful cloud computing adoption by addressing the challenges identified. With the roadmap an evaluation framework that uses the criteria proposed in the roadmap was developed that measures the adherence level to the proposed roadmap.

9.3 Contributions to the Body of Knowledge

The challenges facing cloud computing adoption were identified as the main research area of this project. The motivation for this is the slow adoption of cloud computing by many large organisations such as financial institutions and state or government agencies. Following this, a roadmap for successful adoption of cloud computing and its achievement framework was synthesised. The motivation for development of the roadmap being the need to address the identified challenges and provide organisations with a tool for guidance in adoption cloud computing.

In order to achieve this, an extensive literature review on cloud computing, trust and security issues related to cloud computing, legal and compliance issues and organisational challenges for cloud adoption was conducted. The objective was to understand how organisation perceives cloud computing despite its promised benefits. An extensive exploration of trust models, security standards, regulations on privacy and data protection and the impact of technology on organisation culture, processes and structure were done. The literature revealed that most of the trust and security issues raised originate from the traditional computing environment, while those related to legal and compliance issues related to the complex nature of technology and the rate at which technology changes as opposed to legislation. As to the organisational impact of cloud computing, it was revealed

that little research has been conducted as to the impact of cloud computing to social technical aspects of cloud computing.

Based on the findings from literature review, a survey was prepared which aimed at investigating the main concerns of organisation in adopting cloud computing and also the information assurance practices of vendors. The targeted survey respondents were CEO, CIO, executives, IT strategists among others. And for the survey on information assurance practices vendors were selected based on the publicly available information of the top ten cloud computing vendors. The survey revealed that the greatest concerns were security, privacy, SLA and vendor lock-in. Other concerns were regulatory compliance, application portability and lack of standards. Moreover, the survey showed that these concerns are the same worldwide.

The aim of the research was to develop a roadmap that would assist organisations in leveraging cloud computing through successful adoption. Using the results from literature review and survey, the roadmap for enabling successful adoption of cloud computing was developed. The roadmap is an open framework that can be used in any organisation and for any cloud computing platform and infrastructure as guidance towards successful cloud computing adoption. The roadmap was evaluated by business expert and proved to be applicable in an organisational context.

Following the evaluation of the roadmap, recommendations were drawn, that are key to successful cloud computing adoption project.

Even though time was limited, the results obtained reflect the positive effect of using the roadmap for ensuring successful adoption of cloud computing in an organisation.

9.4 Experimentation, Evaluation and Limitation

The survey conducted as part of this research aimed at investigating the challenges facing cloud computing adoption and vendors' information assurance practices. The survey was conducted in two phases. The first phase involved of online survey and the second phase involved an offline survey of vendors' information assurance practice using publicly available information such as press releases, privacy policies and user agreements/terms of service agreements. The results obtained from phase one of the survey were key to formulation of questions for survey in phase two. The results were also analysed and

compared to survey results from other researches. The results from phase two of the survey helped to analyse the perceptions of cloud customers and whether their reluctance or hesitation in adopting cloud computing based on their perceived challenges were justifiable.

It was possible to synthesise the roadmap by comparing the results obtained from the survey by those obtained from other researches and the findings from the literature review. The reason for the low number of respondents is due to the fact that the survey was conducted during the summer months of July and mid August. Therefore, questionnaire distribution by e-mail was not successful and there were many out-of-office notification emails. However, the survey provided important findings such as, the shift in the key drivers from cost to the need for IT resource scalability and flexibility.

Following the results from literature review and survey a roadmap and its evaluation framework were developed. The roadmap and its framework were then evaluated by Mr. Mwazambe a technical expert, and recommendations for its improvements were given.

9.5 Future Work & Research

Although the technologies underlying cloud computing have existed for nearly sixty years, cloud computing as a computing paradigm has existed for just a few short years. As a result the scope for further research is broad. This section provides some starters for future work and research.

There is need for more case studies to evaluate the roadmap and its framework. This is because in this research it was not possible. These case studies from both successful and unsuccessful projects will help to improve the roadmap and the framework. Another area for further research is that of assessing the social-technical impacts of cloud computing in organisation.

Social-technical impact: the impact of migrating to cloud computing and its effects on the organisational culture, people and their relationships, work performance and system affordances. Research in this area should seek to answer questions such as: how does migrating to cloud affect the current work practices? Will system affordances change and how will they change?

9.6 Conclusion

Chapter 9 presented the overall conclusion of the research carried out and the recommendations for future researchers.

Also the research overview was given where the aim for the research project was given. The research aim was to develop a roadmap that will enable successful adoption of cloud computing by organisations. To achieve this perceived challenges facing organisation in cloud adoption and the information assurance practices of cloud vendors that hinders adoption of cloud computing were identified. The research contribution to knowledge was identified as the developed roadman and its achievement framework.

Research evaluation was presented and the results and recommendation of the evaluation discussed. The chapter also, discussed future research areas. The suggested research areas outlined in this chapter are as follows: business models for cloud computing, the impact of cloud computing to social-technical factors of an organisation, payment models, legal and compliance framework and security and trust issues.

BIBLIOGRAPHY

ABDUL-RAHMAN, A. & HAILES, S. (1997) Using recommendations for managing trust in distributed systems. Citeseer

ABDUL-RAHMAN, A. & HAILES, S. (1998) A distributed trust model. ACM

ABDUL-RAHMAN, A. & HAILES, S. (2000) Supporting trust in virtual communities. Published by the IEEE Computer Society

ABRAMS, M. D. & JOYCE, M. V. (1995) Trusted System Concepts. *Computer & Security,* 14**,** 45-56.

ACREMENT, B. (2010) Elements for Building Trust: Do Your Management Skills Measure Up? marketing times online, http://www.imakenews.com/smei/e_article000051474.cfm, 15/07/2010.

ALCALDE, B., DUBOIS, E., et al. (2009) Towards a decision model based on trust and security risk management. *Information Security 2009***,** 61.

ALUNKAL, B. K. (2003) GRID EIGEN TRUST A FRAMEWORK FOR COMPUTING REPUTATION IN GRIDS. Citeseer

AMAZON (2010) Amazon Web Services Customer Agreement; Amazon.com, http://aws.amazon.com/agreement, 30/06/2010.

ANDERT, D., WAKEFIELD, R., et al. (2002) Trust Modeling for Security Architecture. Santa Clara, CA, Sun Microsystems, INC

ANDREI, T. (2009): Cloud Computing Challenges and Related Security Issues;

ARMBRUST, M., FOX, A., et al. (2009): Above the clouds: A berkeley view of cloud computing [Technical Report]; University of California, Berkeley;

ARTZ, D. & GIL, Y. (2007) A survey of trust in computer science and the Semantic Web. *Journal of Web Semantics,* 5**,** 58-71.

ASSOCIATES, R. (2003) PESTLE Analysis; renewal.eu, www.renewal.eu.com/Renewal_Pestle_Analysis.pdf, 1/4/2010.

AUDUN, J., SANG, et al. (2007) A survey of trust and reputation systems for online service provision. *Decis. Support Syst.,* 43**,** 618-644.

BARBER, B. (1986) *THe Logic and Limit of Trust*, Rutgers University Press.

BARROSO, L. A. & HÖLZLE, U. (2009) *The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines*, Morgan & Claypool.

BHATTACHARJEE, R. (2009) An Analysis of the Cloud Computing Platform. *System Design and Managemet.* Massachussets, Massachussets Institute of Technology

BINGELOW, S. J. (2010):Pro and Cons of Moving to the Cloud;Virtual Data Center E-Zine Vol 21;TechTarget. www.techtarget.com, April

BLAZE, M., FEIGENBAUM, J., et al. (1999) The role of trust management in distributed systems security. *Secure Internet Programming***,** 185-210.

BLAZE, M., FEIGENBAUM, J., et al. (1996) Decentralized trust management, in: Proceedings of IEEE Symposium on security and Privacy. *IEEE Symposium on Security and Privacy.* IEEE

BOEYEN, S., ELLISON, G., et al. (2003) Liberty Trust Models Guidelines. Liberty Alliance Project

BOS, N., OLSON, J., et al. (2002) Effects of four computer-mediated communications channels on trust development. ACM

BRAGG, R. (2008) Cloud Computing: When computers really rule. *Tech News World.*12/12/2009 12/12/2009

BROMILEY, P. & CUMMINGS, L. L. (1995) *Organisation with Trust,* Greenwich, CN, JAI Press.
BSI (2005 a) BS ISO/IEC 27001:2005/BS 7799-2:2005: Information Technology-Security Techniques-Information Security Management Systems-Requirements. British Standards Institution
BSI (2005 b) BS ISO/IEC 27002:2005, BS 7799-1:2005,BS ISO/IEC 17799:200: Information Technology. Security Techniques. Code of Practice for Information Security Management. British Standards institution
BSI (2007) BS 25999-2:2007: Business Continuity Management. Specification. British Standards Institution
BSI (2008) BS ISO/IEC 27005:2008: Information Technology. Security Techniques. Information Security Risk Management. British Standards Institution
BUYYA, R., YEO, C. S., et al. (2008) Market-oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. *10th IEEE Conference on High Perfomance Computing and Communications.* IEEE
BUYYA, R., YEO, C. S., et al. (2009) Cloud computing and emerging IT platforms: Vision, Hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems,* 25**,** 599 - 616.
CARBONE, M., NIELSEN, M., et al. (2003) A formal model for trust in dynamic networks.
CARR, N. (2008) *The Big Switch: Rewiring the World from Edison to Google,* Denver, Colorado, USA, W.W.Norton.
CASTELFRANCHI, C. & FALCONE, R. (2002) Social trust: A cognitive approach. *Trust and deception in virtual societies***,** 55–90.
CATTEDDU, D. & HOGBEN, G. (2009): Cloud Computing: Benefits, risks and recomendations for information security; European Network and Information Security Agency (ENISA);
CHELLAPA, R. (1997) Intermediaries in Cloud-Computing: A new Computing Paradigm. *Cluster:Electronic Commerce*.
CHOW, R., GOLLE, P., et al. (2009) Cloud Computing: Outsourcing Computation Without Outsourcing Control. *1st ACM Cloud Comptuting Security Workshop.* ACM
CLOUDCOMPUTING (2010) Cloud Application Migration; cloudcomputing.sys-con.com, http://www.cloudcomputing.sys-con.com/node/1458739, 30/07/2010.
COHEN, A. K. (1966) *Deviance and Control,* Englewood Cliffs, New Jersey, Prentice-Hall, Inc.
COMSCI (2010) Managing the Cloud: An Even Greater Need for IT Cost Transparency [Industry Whitepaper]. COMSCI.com
CORNELLI, F., DAMIANI, E., et al. (2002) Choosing reputable servents in a P2P network. ACM
CSA (2009) Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance
CSA (2010): Top Threats to Cloud Computing V1.0; Cloud Security Alliance; 14
DALHEIMER, M. & PFREUNDT, F. J. (2009) GenLM: License Management for Grid and Cloud Computing Environments. In *Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID). 9Th IEEE/ACM International Symposium on Cluster Computing and the Grid.* Washington, USA, IEEE Computer Society
DAMIANI, E., PARABOSCHI, S., et al. (2002) A reputation-based approach for choosing reliable resources in peer-to-peer networks. ACM New York, NY, USA

DASH, R. K., RAMCHURN, S. D., et al. (2004) Trust-based mechanism design.
DE ASSUNÇÃO, M. D., DI COSTANZO, A., et al. (2009) Evaluating the cost-benefit of using cloud computing to extend the capacity of clusters. In *HPDC '09: Proceedings of the 18th ACM International Symposium on High Performance distributed computing*. *High Perfomance Distributed Computing HPDC '09.* Munich, Germany, ACM
DELLAROCAS, C. (2003) The digitization of word of mouth: Promise and challenges of online feedback mechanisms. *Management Science,* 49**,** 1407-1424.
DONDIO, P. & BARRET, S. (2007) Computational trust in Web Content quality. *Informatica*.
DUSTIN AMRHEIN, P. A., ANDREW DE ANDRADE, JOE, ARMSTRONG, E. A. B., JAMES BARTLETT, RICHARD BRUKLIS, KEN CAMERON, et al. (2010) Cloud Computing Use Cases White Paper. Version 3.0 ed., Cloud COmputing Use Case Discussion Group
EC (2006) Directive 2006/24/EC: The retention of data generated or processed in connection with provision of publicly available electronic communications services or public communication networks and amending Directive 2002/58/EC. EC
ECONOMIST (2008) Let it rise, A special report on corporate IT. *The Economist.* October 2008 ed.,
ELSALAMOUNY, E., SASSONE, V., et al. HMM-based Trust Model. *Formal Aspects in Security and Trust***,** 21-35.
ELSON, J. & HOWELL, J. (2009) Refactoring Human Roles Solves systems Problems. In *Workshop on Hot Topics in Cloud Computing*. *HotCloud 2009.* San Diego, USA, HotCloud
EU (2006) Directive 2006/24/EC: The retention of data generated or processed in connection with provision of publicly available electronic communications services or public communication networks and amending Directive 2002/58/EC. EC
FALCONE, R. & CASTELFRANCHI, C. (2004) Trust dynamics: How trust is influenced by direct experiences and by trust itself. IEEE Computer Society
FARBER, D. (2008) Oracle's Ellison nails cloud computing; cnet news, http://news.cnet.com/8301-13953_10052188-80.html, 5/06/2010.
FELLOWS, W. (2008) Partly Cloudy, Blue-Sky THinking About Cloud Computing. Whitepaper. 451 Group
FORBES (2010) Seeding the Cloud: Enterprises Set Their Strategies for Cloud Computing [Whitepaper]. Forbes
FORRESTER (2010) Do you Know Wher Your Data Is in the Cloud? Forrester Research Inc, http://www.forrester.com/cloudprivacyheatmap, 14/07/2010.
FOSTER, I., JENNINGS, N. R., et al. (2004) Brain meets brawn: Why grid and agents need each other.
FOX, A. (1976) Beyond Contract: Work, Power and Trust Relations. *The American Journal of Sociology,* 82**,** 239-242.
FRIEDMAN, B., KAHN, P. H., et al. (2000) Trust Online. *Communication of the ACM,* 43**,** 34-40.
GAMBETTA, D. (2000) Can we trust trust. *Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford***,** 213-237.
GEELAN, J. (2009) Twenty-One Experts Define Cloud Computing. *Cloud Computing Journal.* Cloudcomputing.sys-con.com,12/4/2010 12/4/2010

GEFEN, D. (2002) Reflections on the dimensions of trust and trustworthiness among online consumers. *ACM SIGMIS Database,* 33**,** 53.
GNI (2009) Demystifying the cloud: Important opportunities, crucial choices. GNi
GOLBECK, J. & HENDLER, J. (2004a) Accuracy of metrics for inferring trust and reputation in semantic web-based social networks. *Engineering Knowledge in the Age of the SemanticWeb***,** 116-131.
GOLBECK, J. & HENDLER, J. (2004b) Reputation network analysis for email filtering. Citeseer
GOLBECK, J. & HENDLER, J. (2006) Inferring binary trust relationships in web-based social networks. *ACM Transactions on Internet Technology (TOIT),* 6**,** 529.
GOLBECK, J. A. (2005) Computing and applying trust in web-based social networks.
GOLDEN, B. (2009) The Case Against Cloud Computing; CIO, http://www.cio.com/article/print/481668, 02/07/2010.
GOOGLE (2010) Google App Engine Terms of Service; Google.com, http://code.google.com/appengine/terms.html, 30/6/2010.
GRANCE, T. (2010) The NIST Cloud Definition Framework. NIST
GRANDISON, T. & SLOMAN, M. (2000) A survey of trust in internet applications. *IEEE Communications Surveys and Tutorials,* 3**,** 2-16.
GRANDISON, T. & SLOMAN, M. (2002) Specifying and analysing trust for internet applications. Kluwer Academic Pub
GREENBERG, A., HAMILTON, J., et al. (2008) The cost of a cloud: research problems in data center networks. *ACM SIGCOMM Computer Communication Review,* 39**,** 68-73.
GREENE, T. (2009) Cloud security stokes concerns at RSA; Network World, www.networkworld.com/news/2009/042309-rsa-cloud-security.html?hpg1=bn, 16/06/2010.
GREENWOOD, D., KHAJEH-HOSSEINI, A., et al. (2010) The Cloud Adoption Toolkit: Addressing the Challenges of Cloud Adoption in Enterprise. *Arxiv preprint arXiv:1003.3866*.
HAMILTON, B. A. Cloud Computing Security Standards: Evolving from the Classic Data Center Baseline. BAH
HOGBEN, G. & CATTEDDU, D. (2009) Interoperability and Protection: Cloud Computing Benefits, Risks and Recommendations for Information Security. *ENISA Quartely Review.*
HUSTINX, P. (2010) Data Protection and Cloud Computig under EU law; Panel IV: Privacy and Cloud Computing: in. *Third European Cyber Security Awareness Day.* BSA, European Parliament, European Parliament
IBM (2001): Autonomic Computing: IBM's Perspective on the State of Information Technology; IBM; 22
IDC (2009) IDC Enterprise Panel, 3Q09, n=263. IDC
ISACA (2010) COBIT Framework for IT Governance and Control; ISACA, http://www.isaca.org/Knowledge-Center/COBIT/pages/Overview.aspx, 2/4/2010.
ITGI (2007) COBIT 4.1: Framework, Control Objectives, Management Guidelines and Maturity Model. IT Governance Institute (ITGI)
ITU (2005) Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. International Telecommunication Union

JAEGER, P. T., LIN, J., et al. (2009):Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing;First Monday Number 4-5;University of Illinois, Chicago. 12. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171, 27/07/2010
JEFFREY, K. & NEIDECKER-LUTZ, B. (2009): THE FUTURE OF CLOUD COMPUTING: OPPORTUNITIES FOR EUROPEAN CLOUD COMPUTING BEYOND 2010; 66
JENSEN, M. & SCHWENK, J. (2009) On Technical Security Issues in Cloud Computing. *2009 IEEE Conference on Cloud Computing.* IEEE Computer Society
JERICHO (2009) Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration V1.0 (Position Paper). Jericho Forum
JOHNSON-GEORGE, C. & SWAP, W. C. (1982) Measurement of specific interpersonal trust: Construction and validation of scale of assess trust in a specific other. *Journal of Personality and Social Psychology,* 43**,** 1306-1317.
JOHNSON, B. (2008) Cloud Computing is a trap, Warns GNU Founder Richard Stallman; the guardian, www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman, 4/6/2010.
JØSANG, A. & ISMAIL, R. (2002) The beta reputation system. Citeseer
KAGAL, L., FININ, T., et al. (2003) A policy based approach to security for the semantic web, in: Proceedings of the 2nd International Semantic Web Conference. *The SemanticWeb-ISWC 2003.* Springer
KAMVAR, S. D., SCHLOSSER, M. T., et al. (2003) The eigentrust algorithm for reputation management in p2p networks. ACM
KEENE, C., PODDAR, I., et al. (2009) Cloud Quick Start: A Roadmap For Adopting Cloud Computing [White paper]. IBM
KEPHART, J. O. & CHESS, D. M. (2003) The Vision of Autonomic Computing. *Computer Magazine.* January, 2003 ed.,
KHAJEH-HOSSEINI, A., SOMMERVILLE, I., et al. (2010a) Research Challenges for Enterprise Cloud Computing. *Arxiv preprint arXiv:1001.3257.*
KHAJEH-HOSSEINI, A., SOMMERVILLE, I., et al. (2010b) Research Challenges for Enterprise Cloud Computing.
KLEMS, M., NIMIS, J., et al. (2009) *Do Clouds Compute? A framework for estimating value of cloud computing.Designing E-Business Systems. Markets, Services, and Networks*, Springer Berlin Heidelberg.
KNODE, R. (2009) BP Fuels Cloud Computing Interest; trustedcloudservices.com, http://www.trustedcloudservices.com/Individual-Case-Studies/bp-fuels-cloud-computing-interest, 15/02/2010.
KOHL, J. & NEUMAN, C. (1993): The Kerberos network authentication service (v5); Citeseer;
KONDO, D., JAVADI, B., et al. (2009) Cost-Benefit Analysis of Cloud CODlputing versus Desktop Grids. In *Proceedings of the 2009 IEEE International Symposium on Parallel and Distributed Processing*. *2009 IEEE International Symposium on Parallel and Distributed Processing.* IEEE
KRAUTHEIM, F. J. (2009) Private Virtual Infrastructure for Cloud Computing.
KRUKOW, K., NIELSEN, M., et al. (2008) Trust models in ubiquitous computing. *Philosophical Transactions of the Royal Society A,* 366**,** 3781-3793.

KRUKOW, K., NIELSEN, M., et al. (2009) Probabilistic Computational Trust.
LEWIS, J. D. & WEIGERT, A. (1985a) Social atomism, holism, and trust. *The Sociological Quartely,* 26**,** 455-471.
LEWIS, J. D. & WEIGERT, A. (1985b) Trust as a social reality. *Social Forces,* 63**,** 967-985.
LIA, N., WINSBOROUGH, W. H., et al. (2003) Distributed credential chain discovery in trust management. *Journal of Computer Security,* 11**,** 35-86.
LOHR, S. (2007) Google and I.B.M Join in 'Cloud Computing' Research. *The New York Times.*
LUIS, M. V., LUIS, R.-M., et al. (2008) A break in the clouds: towards a cloud definition. *SIGCOMM Comput. Commun. Rev.,* 39**,** 50-55.
MARSH, S. P. (1994) Formalising Trust as a Computational Concept. *Computing Science and Mathematics.* University of Stirling
MARTI, S. & GARCIA-MOLINA, H. (2006) Taxonomy of trust: Categorizing P2P reputation systems. *Computer Networks,* 50**,** 472-484.
MATHER, T. (2010) Let There be Light. *Information Security.* June 2010 ed.,
MATHER, T., KUMARASWAMY, S., et al. (2009) *Cloud Security and Privacy: An Enterprise Perspective on Risk and Compliance,* Sebastopol, CA, O'Reilly Media, Inc.
MAYER, R. C., DAVIS, J. H., et al. (1995) An integrative model of organizational trust. *Academy of Management Review,* 20**,** 709-734.
MCFEDRIES, P. (2008) The Cloud is the Computer; IEEE Spectrum, www.spectrum.ieee.org/computing/hardware/the-cloud-is-the-computer, 15/06/2010.
MCKNIGHT, D. H. & CHERVANY, N. L. (1996): The Meanings of Trust. Technical Report MISRC Working Paper Series 96-04; University of Minesota, Management Information Systems Research Center;
MCKNIGHT, D. H. & CHERVANY, N. L. (2001) The meanings of trust. *Trust in Cyber-Societies-LNAI,* 2246**,** 27-54.
MCKNIGHT, D. H., CUMMINGS, L. L., et al. (1998) Initial Trust Formation in New Organisational Relationships. *Academy of Management Review,* 23**,** 473-490.
MELL, P. & GRANCE, T. (2009a) The NIST Definition of Cloud Computing Version 15. National Institute of Standards and Technology
MELL, P. & GRANCE, T. (2009b) Perspective on Cloud Computing Standards. USA, NIST
MILLER, M. (2008) *CLOUD COMPUTING: Web-Based Applications That Change the way You Work and Collaborate*, Que Publishers.
MIT (2009) Multics; MIT, http://web.mit.edu/multics-history/#history, 11/02/2010.
MUI, L., MOHTASHEMI, M., et al. (2002) A Computational model of Trust and Reputation. *in: Proceedings of the 35th International Conference on Systems Science.*
NEJDL, W., OLMEDILLA, D., et al. (2004) Peertrust: Automated trust negotiation for peers on the semantic web. *Secure Data Management***,** 118-132.
NEUMAN, B. C. & TS'O, T. (1994) Kerberos: An authentication service for computer networks. *IEEE Communications Magazine,* 32**,** 33-38.
NIELSEN, M. & KRUKOW, K. (2003) Towards a formal notion of trust, in: PPDP'03: Proceedings of the 5th ACM SIGPLAN International Conference on Principles and Practice of Declarative Programming. *5th ACM SIGPLAN International Conference on Principles and Practice of Declarative Programming.* ACM Press

NIELSEN, M., KRUKOW, K., et al. (2007) A Bayesian model for event-based trust. *Electronic Notes in Theoretical Computer Science,* 172**,** 499-521.
NURMI, D., WOLSKI, R., et al. (2009) The eucalyptus open-source cloud-computing system. IEEE Computer Society
OASIS (2005a) OASIS eXtensible Access Control Markup Language (XACML) TC; OASIS, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml, 15/07/2010.
OASIS (2005b) OASIS Security Services (SAML); OASIS, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml, 15/07/2010.
OASIS (2007) WS-Trust 1.3; OASIS, http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html, 15/07/2010.
OGC (2010) What is ITIL? Office of Government Commerce, http://www.itil-officialsite.com/AboutITIL/WhatisITIL.asp, 15/07/2010.
OLMEDILLA, D., RANA, O., et al. (2005) Security and trust issues in semantic grids. *in: Proceedings of the Dagsthul Seminar, Semantic Grid:Tthe Convergence of Technologies.*
OPENCROWD (2010) Cloud Landscape; OpenCrowd, www.opencrowd.com/views/cloud.php, 11/06/2010.
OSA (2010) Pattern: Cloud Computing; Open Security Architecture (OSA), http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing, 16/06/2010.
PEARSON, S., MONT, M. C., et al. (2005) Analysis of Trust Properties and Related Impact of Trusted Platforms. Bristol, HP
PIRZADA, A. A. & MCDONALD, C. (2004a) Establishing trust in pure ad-hoc networks. Australian Computer Society, Inc.
PIRZADA, A. A. & MCDONALD, C. (2004b) Kerberos assisted authentication in mobile ad-hoc networks. Australian Computer Society, Inc.
PIRZADA, A. A. & MCDONALD, C. (2006) Trust establishment in pure ad-hoc networks. *Wireless Personal Communications,* 37**,** 139-168.
PLUMMER, D. C., SMITH, D. M., et al. (2009): [Reaearch] Five Refining Attributes of Public and Private Cloud; Gartner;
PRENTICE, B. (2010) Cloud Computing: What it is all About? Gartner
RAGHAVAN, B., VISHWANATH, K., et al. (2007) Cloud Contro with Distributed Rate Limiting. *SIGCOMM '07.* Kyoto, Japan, ACM
REMPEL, J. K., HOLMES, J. G., et al. (1985) Trust in close relationships. *Journal of Personality and Social Psychology,* 49**,** 95-112.
RIEGELSBERGER, J. (2002) THE EFFECT OF FACIAL CUES ON TRUST IN ECommerce SYSTEMS. *Doctoral Consortium, Proceedings of HCI,* 2**,** 234-235.
RISTENPART, T., TROMMER, E., et al. (2009) Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. *CCS'09.* Chicago, Illinois, USA, ACM
ROBINSON, N., GRAUX, H., et al. (2009): [Technical Report] Review of the European Data Protection Directive; Information Commissioner's Office; TR-710-ICO. 82
ROCHWERGER, B., BREITGAND, D., et al. (2009) The reservoir model and architecture for open federated cloud computing. *IBM Systems Journal,* 53.
ROSSEAU, D. M., SITKIN, S. B., et al. (1998) Not so Different After All: A Cross-Discipline View of Trust. *Academy of Management Review,* 23**,** 393-404.

ROTTER, J. B. (1980) Interpersonal trust, trustworthiness, and gullibility. *American Psychologist,* 35**,** 1-7.
SANTOS, N., GUMMADI, K. P., et al. (2009) Towards Trusted Cloud Computing. Max Planc Institute for Software Systems
SASSONE, V., KRUKOW, K., et al. (2006) Towards a formal framework for computational trust. Springer-Verlag
SAVVIS (2010): Rising to the Challenge: 2010 Global IT Leadership Report; SAVVIS; 11
SCANZONI, J. (1979) *Social exchange and behaviour interdependency. I,* New York, Academic Press.
SCHNEIR, B. (2008) The Psychology of Security. schneir.com
SHAPIRO, S. P. (1987) The Social Control of impersonal trust. *American Journal of Sociology,* 93**,** 623-658.
SHEFF, D. (2003) Crank it up; wired.com, www.wired.com/wired/archive/8.08/loudcloud_pr.html, 11/06/2010.
SOTTO, L. J., TREACY, B. C., et al. (2010): Privacy and Data Security Risks in Cloud Computing; The National Bureau of National Affairs, Inc; 15 ECLR 186.
STEWART, K. J. (2003) Trust transfer on the world wide web. *Organization Science,* 14**,** 5-17.
STEWART, K. J. & ZHANG, Y. (2003) Effects of hypertext links on trust transfer. ACM
SWINTON, L. (2004) How to do a SWOT analysis; CSM, http://www.customerservicemanager.com/swot-analysis.htm, 20/2/2010.
THOMPSON, M., JOHNSTON, W., et al. (1999) Certificate-based access control for widely distributed resources. USENIX Association
TONTI, G., BRADSHAW, J. M., et al. (2003) Semantic Web languages for policy representation and reasoning: a comparison of kaos, rei,and ponder, in: Proceedings of the 2003 International Semantic Web Conference. *2003 International Semantic Web Conference.*
USZOK, A., BRADSHAW, J., et al. (2003) KAoS Policy and Domain Services: Towards a description-logic approach to policy representation, deconfliction and enforcement policy, in: the Proceedings of IEEE 4th International Workshop on Plocies for Distributed Systems and Networks. *IEEE 4th International Workshop on Plocies for Distributed Systems and Networks.* IEEE
VIEGA, J., KOHNO, T., et al. (2001a) Trust (and mistrust) in secure applications. *Communications of the ACM,* 44**,** 36.
VIEGA, J., MCGRAW, G., et al. (2001b) *Building secure software: how to avoid security problems the right way*, Addison-Wesley Reading, MA.
VOONA, S. & VENKANTARATNA, R. (2009): Cloud Computing for Banks; Infosys Technologies Ltd;
VOUK, M. (2008) Cloud Computing - Issues, Research and Implementations. *Journal of Computing and Information Technology.*
WANG, L. & LASZEWSKI, G. V. (2008) Scientific Cloud Computing: Early Definition and Experience. *10th IEEE Conference on High Performance Computing and Communications.* Dalian, IEEE
WANG, Y. D. & EMURIAN, H. H. (2005) An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior,* 21**,** 105-125.
WARREN, S. D. & BRANDEIS, L. D. (1890) The Right to privacy. *Havard Law Review,* 4.
WEINHARDT, C., ANANDASIVAM, A., et al. (2009) Business Models in the Service World. *IT Professional.*

WIDMER, D. U. (2009) Cloud Computing - ICT as a Service; Who's Who Legal, http://www.whoswholegal.com/news/features/article/18246/cloud-computing-data-protection/, 27/07/2010.
WILLIAMS, A. (2010) Top 5 Cloud Outages of the Past Two Years: Lessons Learned; ReadWriteWeb, http://www.readwriteweb.com/cloud/2010/02/top-5-cloud-outages-of-the-pas.php, 06/07/2010.
WINSLETT, M., YU, T., et al. (2002) Negotiating trust in the Web. *IEEE Internet Computing,* 6**,** 30-37.
XIONG, L. & LIU, L. (2002) Building trust in decentralized peer-to-peer electronic communities. Citeseer
YANOSKY, R. (Ed.) (2008) *From Users to Choosers: The Cloud and the Changing Shape of Enterprise Authority: In The Tower and the Cloud*, UDUCAUSE.
YU, B. & SINGH, M. P. (2002) Distributed reputation management for electronic commerce. *Computational Intelligence,* 18**,** 535-549.
YU, T. & WINSLETT, M. (2003) Policy migration for sensitive credentials in trust negotiation. *in WPES '03: Proceedings of the 2003 ACM workshop on Privacy in the Electronic Society.* ACM
YU, T., WINSLETT, M., et al. (2001) Interoperable strategies in automated trust negotiation. *8th ACM conference on Computer and Communications Security.* ACM
ZAND, D. E. (1972) Trust and Managerial Problem Solving. *Administrative Science Quartely,* 17**,** 229-239.
ZHENG, J., VEINOTT, E., et al. (2002) Trust without touch: jumpstarting long-distance trust with initial social activities, in: CHI '02:Proceeding of the SIGHI Conference on Human Factors in Computing Systems. *SIGHI Conference on Human Factors in Computing Systems.* ACM Press

APPENDIX A

Questionnaire

This survey questionnaire on Cloud Computing trust, aims to identifying the reasons behind possible engagement of organisation in the cloud computing, the most suitable model of cloud computing, the willingness of the organisation to outsource IT resources to cloud computing, the challenges in building trust, and the main concerns in cloud computing.

Question 1: Please provide the following information

Your Job Title:	-- Please Select One--
Your Role in IT Decisions:	-- Please Select One --
Nature of the Organisation or Industry:	-- Please Select One --

2: Please select the size of your Enterprise or Organisation

☐ 1 - 99 Employees
☐ 100 - 499 Employees
☐ 500 - 999 Employees
☐ 1000 - 4999 Employees
☐ 5000 or Above Employees

Question 3: Please choose the geographical location your enterprise or organisation is located

☐	America (USA and Canada)
☐	Africa
☐	Asia
☐	Europe
☐	Other(Please specify)

Question 4: What are the key drivers for your organisation to adopt cloud computing?

☐	Economies of scale
☐	Flexibility and Scalability of IT resources
☐	Security benefits of cloud computing
☐	Diversification of IT systems and resources
☐	IT resource optimisation
☐	Other (please specify)

Question 5: What would you consider as the most appropriate Cloud computing delivery model for your organisation?

☐	Public- owned and managed by a third party
☐	Private – owned internally

☐	Private – owned by a trusted third party
☐	Community cloud – shared by trusted partners
☐	Hybrid cloud
☐	Federated clouds from various vendors
☐	Other (please specify)

Question 6: What would you consider as the most appropriate cloud computing deployment model for your organisation?

☐	Software-as-a Service(SaaS)
☐	Platform-as-a-Service(PaaS)
☐	Infrastructure-as-a-Service(IaaS)
☐	Other (please specify)

Question 7: What would you consider as the key characteristics for vendor selection?

☐	Company size
☐	Reputation
☐	Number of clients

☐	Physical location of the cloud
☐	Policy statements
☐	Other (please specify)

Question 8: What type of IT/business processes are you willing to outsource to cloud computing?

☐	Human resources management (HR)
☐	Customer relationship management (CRM)
☐	Sales and marketing
☐	Application development
☐	Research and development
☐	Other (please specify)

Question 9: What are the key concerns for trusting cloud computing vendors?

☐	Security practices
☐	Reputation
☐	Information assurance practices
☐	Privacy policy/policy statement

☐	Compliance with industry standards regulations
☐	Other (please specify)

Question 10: What are indicators that a cloud computing vendor is trustworthy?

☐	Compliance with industry standards
☐	Security practices
☐	Company size, location and number of clients
☐	Reputation
☐	Disaster recovery and business continuity plan
☐	Other (please specify)

Question 11: what would you consider as barriers to cloud computing adoption?ssss

☐	Security concerns
☐	Integration issues with existing systems and applications
☐	Loss of control over data and applications

☐	Availability and performance concerns
☐	Regulatory, Compliance and IT governance issues
☐	Other (please specify)

APPENDIX B

Questionnaire 2

This questionnaire is designed to collect information from publicly available information sources such as policy statements, press releases and user agreements, of cloud computing vendors related to information assurance practices of cloud vendors. The aim is to identify how vendors assure clients of security of their offerings through their policy and user agreements.

Vendor Name: _____

Location: _____

Company size:_____

Question 1: What security issues are covered?

Question 2: What regulatory and compliance issues are covered?

Question 3: How is disaster recovery and business continuity addressed?

Question 4: Who is responsible in the case of data loss or breach of privacy?

Question 5: Who is responsible for compliance issues? How are these issues addressed?

Question 6: How are service level agreements contracted?

Question 7: Are there mitigation plans for any security or trust breach? Who is responsible for issues related to forensics and e-discovery?